



Service Definition

Co-Managed Cloud
Advanced & Premier

Contents

1.	Operational Services.....	2
1.1	Service Description.....	2
2.	Service Operations – Advanced & Premier.....	2
3.	ANS Co-Managed Cloud Service – Advanced.....	6
3.1	Operating System (OS) Support.....	6
3.2	Backup.....	6
3.3	Patching (Servers and Databases).....	7
3.4	Containers.....	8
3.5	Azure Site Recovery (ASR)	9
3.6	Firewall	10
3.7	FinOps	10
3.8	Defender for Cloud	11
3.8.1	Cloud Security Posture Management (CSPM)	11
3.8.2	Cloud Workload Protection Platform (CWPP).....	12
4.	Optional Bolt-On Services - Advanced Tier.....	12
5.	Co-Managed Cloud – Premier.....	14
5.1	DevOps.....	14
5.2	Observability.....	14
6.	Optional Bolt-On Services- Advanced Tier.....	16
7.	Incident Management	17
7.1	Priority Clarification.....	17
7.2	Impact Assessment Factors.....	18
7.3	Re-Classification and Escalation.....	18
7.4	Response SLAs & Target Resolution KPIs Exclusions.....	19
7.5	Reporting.....	19
8.	Change Management	19
8.1	Change Risk Assessment Matrix	20
8.2	Change implementation targets Table:.....	20
9.	Service Levels, Key Performance Indicators and Service Credits.....	21
10.	Exclusions.....	22
11.	Customer Responsibilities	23
12.	Assumptions	24
13.	Pre-Requisites.....	25
14.	Partner of Record	25
15.	Partner Admin Link (PAL)	26
16.	Amazon AWS Associated Partner.....	26
17.	Terms and Definitions	27

1. Operational Services

1.1 Service Description

The ANS Co-Managed Cloud service is designed to support the Customer in getting the most out of their cloud investment. The Supplier delivers this by providing technical expertise, governance, management, and reporting to increase operational value, while FinOps and GreenOps insights and automation help to optimise consumption of the Customer's cloud-based product.

This Co-Managed approach allows the Customer to remain in control over all aspects of the cloud environment, while the Supplier performs only the activities identified as included within this Service Definition Document. This makes the service particularly useful for organisations that want to offload technical overhead whilst still maintaining strategic oversight.

The optional Bolt-on Services allow the Customer to consume additional IT services from the Supplier, to further enhance the efficiency and resilience of their cloud operations. Access to a broader range of expert support allows organisations to swiftly respond to and capitalise on innovative technologies, reducing the administrative burden on internal teams.

2. Service Operations – Advanced & Premier

Operations Baseline		
Activities	Service Operations	Service Hours
ANS Glass Portal Access	The Supplier will provide the Customer with access to the ANS Glass Portal providing visibility of Service-related tickets, alerts and performance dashboards.	24 x 7
Problem Management	The Supplier's Problem Management processes are adhered to for Enhancement Requests, Bug Remediation and Root Cause Analysis. The Supplier conducts proactive Problem Management to identify and rectify recurring incidents triggering and trend analysis.	Normal Business Hours
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a platform P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken via the Problem Management process to identify the underlying cause.	Normal Business Hours
Activities	Incident Management	Service Hours
Incident Management	The Supplier is responsible for conducting the Incident Management Process via the ANS Glass Portal, telephone, and remote connection for priority 2-5 support in Normal Business Hours.	Normal Business Hours
Major Incident Management	The Supplier is responsible for conducting Incident management via telephone and remote connection for priority 1 scenario support 24x7x365. Priority escalation to Microsoft Support is also included where appropriate.	24 x 7

Priority Escalation to Vendor for faults	High priority escalation to Vendor through partner channels for priority 1 Business Critical Incident for Public Cloud Platform.	24 x 7
Activities	Change Management & Advisory	Service Hours
Ops Advisory & Architecture Validation	The Supplier will provide validation and design guidance for new projects and applications via a Normal Change.	Normal Business Hours
Run Book Delivery and Automation	Execution of the Supplier and Customer defined event driven tasks/processes for Customer Supported Assets. Event driven script execution of customer and Supplier defined processes.	24 x 7
Task Automation	Automation of repeatable tasks covering resource provisioning/de-provisioning/restarting and modifying of Customer Supported Assets.	24 x 7
Right Sizing	Assess and right-size VMs on request to ensure resource allocation is aligned with workload requirements, optimising performance and resource utilisation .	Normal Business Hours
Cloud Capacity Management	The Supplier will review existing workloads to identify overcommitted/underutilised resources providing recommendations for remediation, detailing associated cost/performance impact.	Normal Business Hours
Instance Modernisation	The Supplier will recommend new instance types that virtual machines can be migrated to provide performance/cost improvements.	Normal Business Hours
Expert Access	The Supplier provides access to expert advice for question/query Service Requests.	Normal Business Hours
Change Advisory Board (CAB) Authority	The Supplier will act as the CAB for all Change Requests relating to Customer Supported Assets that are classified as Normal Changes. Feature Requests are delivered as a Project Change.	Normal Business Hours
Change Management Process	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets. Changes constitute anything that can be completed by the Supplier within a two-hour window.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement an Emergency Change.	24 x 7
Activities	Monitoring & Event Management	Service Hours
Platform Monitoring	The Supplier will monitor the Customer Supported Assets, providing bespoke workflows, thresholds, availability and performance metrics. Access to the Monitoring Solution, including dashboards, will be provided to the Customer via ANS Glass Portal.	24 x 7
Problem Management	ANS Problem Management processes are adhered to for regular event reduction and threshold optimisation.	24 x 7
Activities	Customer Success	Service Hours
Customer Success	The Supplier will provide a Customer Success representative to facilitate delivery of value to the Customer as part of the Managed Service.	Normal Business Hours

Customer Success Architecture	The Supplier will provide access to architectural validation and technical expertise against Customer Supported Assets, with the delivery model determined by the Customer's service tier.	Normal Business Hours
Customer Success Reviews (CSR)	<p>Customer Success Reviews will be conducted at regular intervals and discussed via an engagement between the Supplier and the Customer. The report review will cover the previous period since the last CSR.</p> <p>Where CoE Services are purchased by the Customer, items highlighted in the CSR reports can be used to shape CoE backlogs on instruction from the Customer.</p>	Normal Business Hours
Wave Release/Deprecations Awareness	The Supplier will make the Customer aware of any relevant new/deprecated features relating to any Customer Supported Assets in a timely manner.	Normal Business Hours

Co-Managed Cloud Advanced

3. ANS Co-Managed Cloud Service – Advanced

In addition to the above, the Co-Managed cloud Service at the Advanced tier (Co-Managed Cloud Advanced Service) will include the following:

3.1 Operating System (OS) Support

The OS Support Service helps Customer's spend less time on OS management that doesn't contribute immediately to the overall goals of the Customer's business. This Service aims to provide the Customer with a level of managed OS Support Service, as well as access to Microsoft qualified experts and the Supplier's 24/7 support teams who will proactively review the environment aiming to prevent issues occurring and disruption to business operations.

Activities	Service Operation Baseline	Service Hours
Priority Escalation to Vendor for faults	High priority escalation to Vendor through partner channels for priority 1 Business Critical Incident for OS on Public Cloud Platform.	24 x 7
OS Configuration	Upon a Change Request being submitted via ANS Glass Portal, the Supplier will provide configuration change on the operating system for disk, CPU, RAM & OS.	24 x 7
Change Management & Advisory		
OS Task Automation	Upon a Change Request being submitted via ANS Glass Portal, the Supplier will provision automation of repeatable tasks covering resource provisioning/de-provisioning/restarting, modifying of supported operating system resources and automated event response,	24 x 7
Platform Monitoring	The Supplier will monitor the platform providing Supplier-bespoke workflows, thresholds, availability and performance metrics. Access to the Monitoring Solution will be provided to the Customer via the ANS Glass Portal.	24 x 7
Change Advisory Board (CAB)	Upon a Change Advisory Change Request being submitted via the ANS Glass Portal, the Supplier will act as CAB authority for all changes considered Normal Changes for the Customer Supported Assets. Feature Requests are delivered as Project Changes.	Normal Business Hours

3.2 Backup

Managed Backup is designed to provide resilient protection of Customer workloads by providing expert guidance, configuration, monitoring, and recovery support for backup environments. The Supplier aims to deliver ongoing management of backup policies, systems, and recovery processes to maintain data integrity and availability, helping the Customer safeguard critical assets and restore services when required.

Activities	Service Operation Baseline	Service Hours
Change Management & Advisory		
Change Guidance & Architecture Validation for Azure Backup	Upon a Change Request being submitted via the ANS Glass Portal, the Supplier provides access to Change Advisory for: <ul style="list-style-type: none"> Backup Architecture & Configuration Backup Policy Validation Backup Design 	Normal Business Hours

Expert Access	The Supplier provides access to expert advice for question/query Service Requests relating to the backups.	Normal Business Hours
Backup Setup & Configuration	Upon a Change Request being submitted via the ANS Glass Portal, the Supplier will setup and configure new backups.	Normal Business Hours
High Availability & Recovery		
Backup & Recovery	Upon a Change Request being submitted via the ANS Glass Portal, the Supplier will help recover from a backup.	Normal Business Hours
Test Backup Restores	Upon a Change Request being submitted via the ANS Glass Portal, the Supplier will test backup restores of Customer Supported Assets up to once quarterly.	Normal Business Hours
Monitoring & Event Management		
Performance Tuning and Diagnostics	The Supplier will periodically agree to help the Customer identify optimisations, upgrades or changes that can help the Customer's backups achieve better and more consistent performance.	Normal Business Hours
Platform Monitoring	The Supplier will provide additional monitoring relating to Azure Backup and respond to alerts via Incident Management Processes for the following: <ul style="list-style-type: none"> • Overrunning Jobs • Failures 	Normal Business Hours

3.3 Patching (Servers and Databases)

The Co-Managed Patching Service is designed to provide the Customer with a consistently configured environment that is secured against known vulnerabilities in the Customer's Operating System. Operating System patching requires a high standard of maintenance and administration to deliver patch compliance across the Customer's Operating System estate, as well as flexibility during periods of growth and change.

The Co-Managed Patching Service leverages a number of tools to enable patch compliance of server endpoints across Azure and AWS, as well giving the Customer access to the Suppliers experts to tailor-make workflows for scheduling and handling of automated patch distribution to servers.

Activities	Service Operation Baseline	Service Hours
Patch Management	The Supplier shall patch Customer Supported Assets in line with the agreed schedule. Assets are grouped in cycles, and the process is repeated on an agreed cadence. The Supplier will provide a monthly patch status report of all Assets within the patching cycle under the Service upon request. In the event of an urgent zero-day patch being released, the Supplier will push out a patch via an Emergency Change process upon agreement from the Customer.	24 x 7
Platform Monitoring	The Supplier will monitor the platform providing Supplier bespoke workflows, thresholds, availability and performance metrics. Access to the Monitoring Solution will be provided to the Customer via ANS Glass Portal.	24 x 7

Container Patching	Where the Customer is running containerised workloads, routine patching of container infrastructure will come in-scope of ANS Co-Managed Patch Service inclusive of the underlying host OS and the Kubernetes control plane.	Normal Business Hours
--------------------	--	-----------------------

3.4 Containers

The Co-Managed Containers Service is designed to provide a secure and resilient platform for running containerised workloads, allowing the Customer to focus on application delivery rather than platform management. The Service offers access to container Supplier experts who design, operate, and continually improve Kubernetes environments. The Service focuses on reliability, security, and best practice governance so the Customer can be confident in the stability and effectiveness of their container platform.

Activities	Service Operation Baseline	Service Hours
Platform Services	The Supplier will manage the cluster ingress capability as a shared platform service, using a cloud native ingress controller and periodically as agreed provide recommendations on security and operational standards, providing routing, load balancing and security. The Supplier will seek to ensure automatic certificate rotation takes place and is responsible for maintaining, availability and scaling.	Normal Business Hours
Cluster Operations	The Supplier will provide management of the Kubernetes platform, designed to deliver security, stability, and scalability. The Supplier will implement upgrades and security patches of the control plane, nodes and platform services as per an agreed schedule. The Supplier will configure automated scaling.	Normal Business Hours
Expert Access	The Supplier provides access to expert advice relating to questions and query Service Requests relating to YAML and helm charts configuration, setup of container images and use of secrets.	Normal Business Hours
Infrastructure	The Supplier will create, configure and manage the underlying infrastructure components that the Kubernetes deployment requires upon a request being submitted via the ANS Glass Portal.	Normal Business Hours
Routine Maintenance	The Supplier will perform patching and upkeep of the database environment inclusive of applying security patches and updates to database software on an agreed schedule.	Normal Business Hours
Container Monitoring	<p>The Supplier will provide monitoring of the Kubernetes deployment:</p> <ul style="list-style-type: none"> Node level performance, CPU, Memory and Disk Cluster level performance, CPU, Memory and Disk Pod Status <p>Access to the Monitoring Solution will be provided to the Customer via the ANS Glass Portal.</p>	24 x 7

3.5 Azure Site Recovery (ASR)

The Co-Managed Azure Site Recovery (ASR) Service is designed to support the Customer's disaster recovery capability for in-scope Azure Site Recovery protected assets. The Service provides expert guidance, configuration, monitoring, recovery plan management, and support for failover and recovery activities, while the Customer retains responsibility for its wider business continuity and disaster recovery strategy, governance, and decision-making.

Activities	Service Operation Baseline	Service Hours
High Priority Recovery	The Supplier will commit to ASR recovery of Customer Supported Assets upon a priority 1 (P1) Incident being raised with the Supplier and an Emergency Change Request from the Customer.	24 x 7
Change Guidance & Architecture Validation for Azure Site Recovery	The Supplier provides access to Change Advisory upon a request being submitted via the ANS Glass Portal for: <ul style="list-style-type: none"> Azure Site Recovery architecture & configuration Azure Site Recovery policy validation Azure Site Recovery design 	Normal Business Hours
Expert Access	The Supplier provides access to expert advice for question/query Service Requests relating to ASR.	Normal Business Hours
ASR Setup & Configuration	The Supplier will setup and configure new recovery plans via the Change Management Process to standard specifications and then customise settings to suit the Customer's requirements.	Normal Business Hours
Patch Management	The Supplier will install Microsoft released Azure Site Recovery updates on an agreed schedule to ASR appliances where required.	Normal Business Hours
Recovery Plans	The Supplier will setup recovery plans and help recover/failover protected resources upon a Customer request being submitted via the ANS Glass Portal.	Normal Business Hours
Test Recovery Plans	The Supplier will test recovery plans of Customer Supported Assets up to once quarterly upon a Change Request being submitted by the Customer via the ANS Glass Portal.	Normal Business Hours
Platform Monitoring	The Supplier will provide additional monitoring relating to ASR and respond to alerts via Incident Management Processes for the following: <ul style="list-style-type: none"> Replication and Failover Health Protection Status Agent Status Access to the Monitoring Solution will be provided to the Customer via the ANS Glass Portal.	24 x 7
Performance tuning and diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customer's replication achieve better and more consistent performance.	Normal Business Hours

3.6 Firewall

The Co-Managed Firewall Service provides expert configuration, management, and ongoing monitoring of the Customer's firewall environment per the table below. The Supplier handles core tasks such as access control, security policy updates, patching, and high availability configuration, while the Customer retains full visibility and control of the firewall. With 24x7 monitoring for performance, threats, and system health, the Service aims to keep the Customer's firewall estate secure, optimised, and compliant—without adding operational burden to the Customer's internal teams.

Co-Managed Firewall		
Activity	Change Management & Advisory	Service Hours
Configuration & Management	Upon a request being submitted via the ANS Glass Portal, the Supplier will provide configuration changes to the Azure Firewalls.	Normal Business Hours
Activity	Monitoring & Event Management	Service Hours
Firewall Monitoring	The Supplier will provide additional monitoring relating to the Azure firewalls, including Supplier bespoke workflows, thresholds, availability and performance metrics. Access to the Monitoring Solution will be provided to the Customer via the ANS Glass Portal.	24 x 7

3.7 FinOps

FinOps provides the Customer with structured financial governance across their cloud estate, combining expert insight, tooling, and best practice frameworks to improve cost efficiency and operational accountability. Through continuous visibility, optimisation recommendations, and collaborative cost management practices, the Service helps the Customer make informed decisions, control cloud spend and maximise the value of their public cloud spend.

Activity	Service Operation Baseline	Service Hours
FinOps	<p>The Supplier utilises the FinOps operational framework to review the value derived from public cloud technologies while maintaining a balance with performance and reliability, steering a cultural practice internally and within the Customer's organisation.</p> <p>The Supplier uses cost management tools to track and analyse spending, allocate costs to business units/products and to identify cost saving opportunities on behalf of the Customer.</p> <p>Access to the FinOps solution will be provided to the Customer via the ANS Glass Portal.</p>	Normal Business Hours

3.8 Defender for Cloud

Defender for Cloud is designed to provide a core capability that continuously monitors and assesses the security configuration of cloud environments across Azure, AWS, and GCP. It provides real-time visibility of assets, identifies misconfigurations and vulnerabilities, and offers actionable guidance to help organisations strengthen their security posture, improve compliance, and reduce risk.

By delivering insights, vulnerability management, and a security score that reflects cloud maturity, Defender for Cloud gives customers a simple but highly effective way to understand and improve their cloud security foundations.

3.8.1 Cloud Security Posture Management (CSPM)

CSPM is a security solution that continuously monitors and assesses the Customer's Cloud providing insights relating to the security posture across Azure, and AWS to allow Customers to prioritise their actions.

Activities	Service Operation Baseline	Service Hours
Regulatory Compliance Management	The Supplier will manage compliance standards in line with the Customers regulatory requirements, configuring standards, producing reports, tracking historical compliance and making recommendations to align to compliance controls.	Normal Business Hours
Defender for Cloud Policy Management	Upon request and following Change Management processes, the Supplier will configure security policies across the platform. These policies will drive recommendations and identify resources that violate the security policies.	Normal Business Hours
Security Posture	The Supplier will regularly review the Defender for Cloud security posture and provide recommendations to improve the secure score and reduce unhealthy resource, where applicable.	Normal Business Hours
Attack Path Analysis	The Supplier will validate whether exposures are reachable and highlight threats to the Customer. The Supplier will provide remediation guidance to break attack paths and strengthen overall cloud security across resources.	Normal Business Hours
Cloud Security Explorer	The Supplier will provide guidance on usage and query creation advice related to Cloud Security Explorer to find security risks.	Normal Business Hours
AI SPM	The Supplier will provide guidance on the AI SPM within the Defender for Cloud Platform, which assesses the security posture of the scanned AI workloads.	Normal Business Hours
Activities	Incident Management	Service Hours
Security Alerts	The Supplier will monitor and respond to security alerts generated by CSPM tooling for in-scope Customer Supported Assets in line with Incident Management processes.	24 x 7

3.8.2 Cloud Workload Protection Platform (CWPP)

CWPP is a cybersecurity solution providing insights and alerts across cloud environments where there is a connection to physical servers, serverless functions, virtual machines, containers and platform-as-a-Service resources, to allow customers to prioritise their Security Posture actions.

Activities	Service Operation Baseline	Service Hours
Workload Protection Configuration	<p>The Supplier will provide expert guidance and support around the configuration of workload protection plans and capabilities within Microsoft Defender for Cloud.</p> <p>Upon request, the Supplier will carry out configuration changes to the Workload Protection plans.</p>	Normal Business Hours
Cost Optimisation	<p>The Supplier will review the cost of the Customer's Defender services and make recommendations for how to optimise costs through resource management and Defender commit units.</p> <p>Upon request, the Supplier will provide cost estimation workbooks to assess the impact of enabling each Defender plan.</p>	Normal Business Hours
Defender for Servers	The Supplier will monitor for security alerts and respond to them via Incident Management process, offering remediation advice and Change Management where appropriate.	Normal Business Hours
Workload Protection Remediation	The Supplier will work with the Customer to address vulnerabilities and misconfigurations identified by the Defender workload protection plans, assessing and prioritising recommendations for the Supplier or the Customer to implement.	Normal Business Hours

4. Optional Bolt-On Services - Advanced Tier

The Customer has the option to consume additional Services to the Co-Managed Cloud Advanced Service where relevant to their business requirements. The terms outlined in this Service Definition will also apply as a minimum baseline for any Bolt-On Services provisioned for the Customer.

Where a Bolt-On Service is purchased in addition to the Co-Managed Cloud Advanced Service, the specific terms, activities, exclusions, responsibilities, assumptions, and pre-requisites relating to the Bolt-On will be outlined in an Annex Document. These are in addition to the terms outlined in this document.

Bolt-On Services applicable for the Co-Managed Cloud Advanced Service are available here: [Service Definitions | ANS Service Definitions](#)

Co-Managed Cloud Premier

5. Co-Managed Cloud – Premier

The Co-Managed Cloud Premier Service includes capabilities within the Advanced Tier as well as the following additions:

5.1 DevOps

DevOps is designed to provide structured support for the Customer's infrastructure and delivery pipelines, helping to improve consistency, control, and operational efficiency across in-scope DevOps activities. The Service provides expert guidance, framework management, optimisation, and ongoing oversight of supported pipeline components, while enabling the Customer to maintain visibility and control of their application delivery processes.

Activities	Service Operation Baseline	Service Hours
IaC standards	The Supplier will maintain stability along with Infrastructure as Code (IaC) delivery processes for any pipeline that have already been prebuilt and onboarded as a Customer Supported Asset in scope of the DevOps Service.	Normal Business Hours
GitOps and Drift Detection	For all Customer Supported Assets onboarded into the Service; GitOps and automated Code Drift detection aims to ensure that every Change is controlled, auditable, and continuously aligned to the intended state, reducing risk and maintaining platform consistency at scale.	Normal Business Hours
Pipeline Optimisation	The Supplier will define best practice GitOps processes for Pull Request workflows, approvals, commit patterns and cost control approval gates in pipelines.	Normal Business Hours
CI/CD Pipeline	The Supplier will monitor pipeline runs and identify and notify the Customer of any failures as well as maintaining the pipeline framework and toolsets.	Normal Business Hours
Customer Success	The Supplier will provide health reporting for Infrastructure as Code relating to recommendations for Code Drift remediations, and performance enhancements.	Normal Business Hours
Expert Access	Technical capability provided by the Supplier to provide architectural validation and technical expertise.	Normal Business Hours

5.2 Observability

Observability is designed to provide the Customer with a single portal that enhances visibility of in-scope services, applications, and infrastructure as well as the Customer's out-of-scope services through centralised monitoring, alerting, logging, and service-level insights. The Service provides expert configuration, dashboarding, anomaly detection, and reporting capabilities to help the Customer identify issues more quickly, improve operational awareness, and maintain informed oversight of service performance and health.

Activities	Service Operation Baseline	Service Hours
Platform Monitoring	The Supplier will onboard the Customer's Unsupported Assets into the Monitoring Solution into a dedicated group. The Supplier will monitor the Customer's Unsupported Assets, providing bespoke workflows, thresholds, availability and performance metrics. Alerting related to enhanced visibility and Customer's Unsupported Assets is routed directly to the Customer and access to the Monitoring Solution, will be provided to the Customer via the ANS Glass Portal.	24 x 7
Monitoring Dashboard Access and Configuration	The Supplier will provide access to monitoring dashboards and will create dashboards for Customer Supported Assets upon request.	Normal Business Hours
Alert Hygiene Reviews	The Supplier will perform monthly optimisations to monitoring configuration to minimise unnecessary event noise.	Normal Business Hours
Expert Access	The Supplier provides access to expert monitoring engineers for guidance on feature capability and usage.	Normal Business Hours
Access to Training	The Supplier provides access to a training portal and materials relating to the relevant observability features.	Normal Business Hours
Activities	Available Capabilities	Service Hours
Observability Services	The Supplier will provide observability capabilities for Customer Supported Assets, delivering visibility of availability, performance, utilisation and operational health across infrastructure, cloud services, applications and supported SaaS platforms. Capabilities may include service availability monitoring, application performance monitoring, synthetic transaction monitoring and end-to-end service health visibility.	24 x 7
Operational Intelligence	The Supplier will aim to periodically provide event correlation, analytics, anomaly detection and service-level insights to identify abnormal behaviour, surface actionable operational intelligence and accelerate incident detection, investigation and response activities.	24 x 7
Operational Automation	The Supplier may utilise diagnostic, investigative and automated response capabilities to enrich alerts, provide additional operational context and execute approved remediation actions, reducing manual effort and improving incident resolution times.	24 x 7
Sustainability Reporting	Upon request, the Supplier will provide sustainability reporting and analytics for onboarded resources, including visibility of carbon emissions, carbon intensity, resource consumption and environmental impact metrics where supported by available data sources.	Normal Business Hours

6. Optional Bolt-On Services- Advanced Tier

The Customer has the option to consume additional Services to the Co-Managed Cloud Premier Service where relevant to their business requirements. The terms outlined in this Service Definition will also apply as a minimum baseline for any Bolt-On Services provisioned for the Customer.

Where a Bolt-On Service is purchased in addition to the Co-Managed Cloud Premier Service, the specific terms, activities, exclusions, responsibilities, assumptions, and pre-requisites relating to the Bolt-On will be outlined in an Annex Document. These are in addition to the terms outlined in this document.

Bolt-On Services applicable for the Co-Managed Cloud Advanced Service are available here: [Service Definitions | ANS Service Definitions](#)

7. Incident Management

7.1 Priority Clarification

The Supplier will assign a Priority Level to each Incident based primarily on impact, specifically, the number and criticality of Users, Sites, or systems that are Down or Affected, as set out in the table below. Response SLA and Target Resolution KPI run within Normal Business Hours unless the relevant row states otherwise.

Priority	Impact / Scope	Response SLA	Target Resolution KPI	Specialist Review	Escalation Manager	Escalation Director	Notification
P1 Critical	Total outage. All Users at a Site, or Users of a Critical System, are completely unable to work and no Workaround is available.	30 minutes	4 Normal Business Hours	1 hour	Immediate	Immediate	Hourly email
P2 High	Partial outage. A Department, a defined group of Users, or a Site is Affected, or a Critical System is impaired; a limited Workaround may exist.	1 Business Hour	1 Business Day	2 Normal Business hours	4 Normal Business hours	None	ANS Glass Portal
P3 Medium	Single User Down or Affected, or a non-critical system is impaired; the User can continue to perform some or all of their role via a Workaround.	4 Business Hours	10 Business Days	1 Business Day	2 Business Days	None	ANS Glass Portal
P4 Low	No operational impact. Cosmetic issues, general how-to questions, minor requests, or planned change requests.	1 Business Day	30 Business Days	Never	Never	None	ANS Glass Portal
P5 Very Low	At this priority level we will provide answers to low priority questions during normal business hours.	2 Business Day	30 Business Days	Never	Never	None	ANS Glass Portal

For an Incident, "Response" is the time from when the ticket is first logged within ANS Glass Portal to the time that the Supplier responds whether via an email, ANS Glass Portal update, telephone call or in person.

For the detailed process flow see the current Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

From the time of Response until resolution, updates shall be provided to the named contacts and/or escalation contacts on the Customer account by email or ANS Glass Portal updates at such frequencies as set out in the table above.

Where the Supplier needs to consult with third parties or Vendors to assist with problem resolution, the Supplier will suspend the 'Target Resolution KPI' until the problem is handed back to the Supplier.

Target Resolution KPIs in this SDD are service level objectives, not guarantees, and are measured to restoration of service or implementation of a Workaround, whichever occurs first, unless the parties agree that a permanent fix is required to close the ticket.

7.2 Impact Assessment Factors

In determining whether an Incident is classified as Down or Affected, and the number of Users in scope, Supplier will take into account:

1. the number of Users unable to perform their role, expressed both as an absolute number and as a proportion of the relevant Site or Department;
2. whether the affected system, application, or infrastructure is designated a Critical System;
3. whether a Workaround exists and, if so, the extent to which it restores normal functionality;
4. whether the Incident affects a single named individual whose role has been pre-designated by Customer as business-critical (a "Designated VIP User"), in which case the Incident may be classified at the next higher Priority Level notwithstanding that only one User is Down or Affected; and
5. any wider business impact notified by the Customer at the time the Incident is logged, including safety, compliance, or regulatory consequences.

The Customer is responsible for providing accurate and complete impact information when logging an Incident and throughout the Incident Management Process. The Supplier may classify or re-classify the Incident based on the information reasonably available to it at the relevant time.

7.3 Re-Classification and Escalation

Either party may request that an Incident be re-classified where the scope of impact changes after initial logging, for example, where a P3 Incident affecting a single User is found to affect an entire Department, or where a Workaround initially available for a P2 Incident ceases to function. The Supplier will notify the Customer in writing, including by ticket update, of any change in Priority level.

P1 Incidents will be escalated internally by Supplier to senior engineering and management resources immediately upon classification, and Supplier will provide the Customer with status updates at intervals of no more than 1 Business Hour until the Incident is resolved or downgraded.

7.4 Response SLAs & Target Resolution KPIs Exclusions

The Response SLAs and Target Resolution KPIs in this SDD do not apply, and the applicable clock will be paused, where:

1. the Incident arises from a cause outside Supplier's reasonable control, including a Force Majeure Event as defined in the Contract;
2. the Supplier is awaiting Customer information, access, approval, instruction, or action, or a third-party vendor action, which is reasonably required to progress diagnosis or resolution;
3. the Incident relates to hardware, software, or infrastructure not supported by Supplier under the Contract; or
4. the Incident is reported outside the Normal Business Hours applicable to its Priority Level, in which case the applicable clock will commence at the start of the next Business Day, unless 24/7 coverage has been separately agreed in writing.

7.5 Reporting

The Supplier will maintain records of Incident classification, Response SLAs, and Target Resolution KPIs for each ticket and will make a summary report available to Customer on a regular basis, or on reasonable request, showing performance against the targets set out in this SDD.

8. Change Management

All Changes require a Change Request Form to be completed on ANS Glass Portal and submitted detailing the required Change. The Supplier will reject unapproved or incomplete Change Request Forms.

Changes will follow the Change Management Process as defined in the Managed Services Handbook. It should be noted that Emergency Changes will only be carried out in the event of a P1 scenario (either pro-active or reactive) as identified in the table above and/or a major Security Incident where the Supplier deems appropriate.

The Supplier shall be entitled to charge for changes where: (i) the Supplier reasonably considers that the change will require more than two hours of effort to implement; (ii) the change would materially increase the Supplier's or the Customer's risk or liability; or (iii) the change would involve an increase in the third party costs associated with the Services. Any such charges shall be agreed in writing by the Parties.

8.1 Change Risk Assessment Matrix

Impact on Service	High	Significant 3 CR3	Major 2 CR2	Critical 1 CR1
	Medium	Minor 4 CR4	Significant 3 CR3	Major 2 CR2
	Low	Candidate for Standardisation 5 CR5	Minor 4 CR4	Significant 3 CR3
		Low	Medium	High
Probability of Negative Impact Until Change is Successfully Completed				

8.2 Change implementation targets Table:

Change Type	Implementation Start Date
Normal CR1	1 Working Day from CAB Approval
Normal CR2	2 Working Days from CAB Approval
Normal CR3	3 Working Days from CAB Approval
Normal CR4	4 Working Days from CAB Approval
Normal CR5	5 Working Days from CAB Approval
Normal CR6	Project Changes (Informational and Approval only)
Standard	Change to be completed within 4 Working days from logging on to the ANS Glass Portal
Emergency	Change to be completed in conjunction with Incident Management Process (P1)

Emergency Changes are dealt with in conjunction with the Incident Management Process; further details of this and all other change types are detailed within the Managed Services Handbook.

Standard Changes and Emergency Changes to the Service within the scope of the Contract will be completed by the Supplier at no additional cost.

9. Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents responded to within 30 minutes – 24 x 7 Service Hours.	100%	1st Incident missed response time – 5% Service Credit 2nd Incident missed response time – 10% Service Credit
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.	Service credits apply from 2 nd failure within a calendar month	1 st Incident missed response time – 0% Service Credit 2 nd Incident missed response time – 5% Service Credit 3 rd Incident missed response time – 10% Service Credit
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.	80%	<80% - 5% Service Credit
P4 Incidents	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5 Incidents	100% of Incidents responded to within 2 Working Days.	None	No Service Credit
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution	None	No Service Credit
CR1 Change	100% of Changes start implementation within 1 Working Day from CAB Approval	100%	1 Change missed implementation time - 5% Service Credit 2 Changes missed implementation times - 10% Service Credit
CR2 Change	90% of Changes start implementation within 2 Working Days from CAB Approval	85%	5% Service Credit

CR3 Change	90% of Changes start implementation within 3 Working Days from CAB Approval	None	No Service Credit
CR4 Change	90% of Changes start implementation within 4 Working Days from CAB Approval	None	No Service Credit
CR5 Change	90% of Changes start implementation within 5 Working Days from CAB Approval	None	No Service Credit
Standard Change	100% of Changes implemented within 4 Working Days	90%	5% Service Credit

Service Credits are calculated as a percentage of the monthly Baseline Charges for the relevant Service, and in any event, shall not exceed 10% of the relevant Baseline Charge in the month that the Service Credit arose. Where a Service Credit is due it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

10. Exclusions

Without prejudice to the other terms of the Contract, the following shall not form part of the Services, subject to any express agreement otherwise in the Quotation or any Change.

- Issues resulting from misconfiguration by the Customer outside of the Demarcation Zone resulting in impact to the Customer's Supported Assets.
- Issues resulting from failures in maintenance/administration by the Customer outside of the Demarcation Zone resulting in impact to the Customer Supported Assets.
- Issues resulting from unauthorised access by the Customer of Customer Supported Assets.
- Issues within, or which are caused by the Customer's code.
- Issues arising within, or attributable to, the Customer's code, custom solutions, intellectual property (including Infrastructure-as-Code (IaC) or other programmatic code), or any bespoke workflows operating outside the defined Demarcation Zone.
- Issues created by the Customer making changes to the solution that impacts the ability of the Supplier to deliver the Service.
- Any issues caused by negligence on the part of the Customer, its employees, servants or agents
- End user or 1st line support.
- Technical advice to discuss account specific details including technical advice to any persons not listed as a named contact.
- Failure to meet the SLA due to outage(s) of the public cloud provider (e.g. Microsoft, or AWS).
- Normal Changes requiring more than 2 hours of implementation time are excluded from the Service and will be subject to Additional Service Charges.
- Project Changes (Normal CR6) are excluded from the Service and will be subject to Additional Service Charges. Project Changes are recorded within ANS Glass Portal for informational and approval purposes only.
- Emergency Changes that are not a direct output of a priority 1 incident may be subject to Additional Service Charges e.g. poor planning from a Customer managed project.
- Existing compromises of the Customer infrastructure prior to being migrated and live in service with the Supplier will be treated as a chargeable project to remediate in order to be accepted into service.

- o. Terms for any additional support services provided by the Supplier to the Customer are not included in this Service.
- p. Applications without accurate services information for on-boarding to the Service will be removed from scope and excluded from on-boarding.
- q. Escalation to Microsoft Premier Support is limited to Major Incidents, subject to Major Incident manager approval. Escalation of Sev B or lower cases is subject to Additional Service Charges.
- r. Management of Server roles & features, including active directory is deemed as out of scope of the OS Support Service.
- s. Managed OS is limited to supported versions of Windows Server only. Desktop operating systems are out of scope of Managed OS.
- t. Windows Server upgrades are out of scope of Managed OS.
- u. Service Desk support is confined to the monitoring as a service platform and excludes any Customer operating system or application.
- v. Alerts relating to any of the observability under the Premier tier are routed directly to the Customer who is responsible for alert response.
- w. Remediation of Customer caused Code Drift is subject to Additional Services Charges.

The Services are co-managed services, meaning that the Customer retains ultimate control, ownership and responsibility for the Customer Supported Assets and for its overall information technology estate. Without limiting the Supplier's obligation to provide the Services described in this document in accordance with the Contract, the Supplier shall not be liable for any loss, liability, cost or expense that arises as a result of the functioning, performance, configuration or administration of the Customer Supported Assets, any related data, information workflows or decisions, or the Customer's use or management of the same.

11. Customer Responsibilities

The following Customer responsibilities apply to the provision of the Services. Failure to comply with these responsibilities may affect the Supplier's ability to deliver the Services in accordance with this Service Definition, including achievement of any applicable Service Levels. These responsibilities include but are not limited to:

- a. The Customer shall have an established end user support function that may be validated by the Supplier.
- b. Where required, the Customer shall make available appropriately skilled employed persons while an Incident is being managed.
- c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
 - a. Affected Services
 - b. Business impact
 - c. Number & type of users affected
 - d. Recent changes on Customer's Supported Assets (regardless of perceived impact)
 - e. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected; and
 - f. The Customer shall check LED status of equipment where required onsite.
- d. The Customer shall provide full administrative access to the Supplier to all the services and systems outlined in the Impact Assessment and any subsequently identified services and systems or provide persons with adequate access to allow investigations to proceed.
- e. The Customer is required to ensure that all Customer Supported Assets are appropriately licensed and have Supplier recommended hardware and third party Vendor support in place.
- f. The Customer is responsible for all configuration backups outside of the Customer Supported Assets without exception.
- g. The Customer is responsible for all data and configuration backups without exception. The Supplier does not backup any Customer Data.
- h. The Customer is responsible for applications not installed by the Supplier.
- i. The Customer is responsible for completing a Change Request in accordance with the Change Management Process.
- j. The Customer shall ensure that all relevant Customer employees have access to and have read the Managed Services Handbook.

- k. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier).
- l. The Customer shall ensure 24x7x365 availability of a suitable escalation contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions.
- m. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer's Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
- n. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Supported Assets and/or Supplier assets from the address specified in the Quotation. Any Asset that has been moved without notification to ANS will be subject to Additional Service Charges.
- o. The Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any SLA or Service Credits for Business Critical Incidents raised via email.
- p. The Customer must be able to provide the Supplier with accurate application and services information in order for the Supplier to successfully on board the Service.
- q. The Customer will ensure adequate anti-virus protection software is installed on the monitoring collector or otherwise request that the Supplier provide this at service on-boarding.
- r. The Customer will be responsible for the responding to alerts in the Defender for Cloud platform for any non-Azure Native devices out of the scope of the Service.
- s. Submit all Service Requests to the Supplier's Service Desk, by telephone or electronically in the ANS Glass Portal by one of the designated named Customer's contacts.
- t. Attend meetings scheduled at mutually convenient times.
- u. Inform the Supplier, with a minimum of 5 Working Days' notice, of any change that may impact the operation of the Service.
- v. Update the Supplier of changes to nominated individuals on the Customer account and associated contact details.

12. Assumptions

The Services are provided on the basis of the following assumptions. If any of these assumptions prove to be incorrect or cease to apply, the Supplier may need to review the scope of the Services, the applicable Service Levels, and/or any charges:

- a. All Customer Supported Assets and production Vendor accounts (as relevant) within the Demarcation Zone within the Contract are covered by a valid software maintenance and support agreement in line with applicable Service Levels.
- b. All Customer Supported Assets are in a valid supported configuration at the Services Commencement Date.
- c. All Customer specific pre-requisites have been completed before the Services Commencement Date.
- d. The Customer will provide a suitable specification platform, operating system for the monitoring collector server.
- e. The Customer will provide resource to work with the Supplier to on board the Service.
- f. Application Code is the sole responsibility of the Customer
- g. SQL patching requires a routine maintenance window for automated patching.
- h. The Supplier reserves the right to restrict utilisation of the Customer Success Architect capability to 10 hours per calendar month.
- i. The Supplier reserves the right to vary this Service Definition in the event of legislative change to the extent required to comply with law or such that the Supplier remains a deployer under current legislation.
- j. Any activities required to bring services up to the expected standard shall be subject to Additional Service Charges.
- k. Any applicable SMS based charges will be charged separately to Customer monthly in arrears.
- l. The Service is provided on the assumption that the Customer will maintain and provision licensing at levels reasonably proportionate to the size, scale, and consumption profile of the Customer's estate. Any usage, consumption, or licensing requirement that exceeds the levels reasonably anticipated for the contracted Service may be deemed outside fair usage and may be subject to Additional Service Charges.

- m. As part of the Service, ANS will include several component elements with include usage bands. These usage bands will be confirmed during the Service onboarding and where the Customer exceeds these allowances, Flex Charges may be incurred to cover the cost of the over usage.
- n. The Supplier will provide expert advice around onboarding non-Azure servers into the Defender for Cloud platform and guidance around plan usage.
- o. The Supplier reserves the right to restrict utilisation of the Customer Success Architect capability to 10 hours per calendar month.
- p. The Service is provided subject to an acceptable use limit. The Customer may be liable for some Additional Service Charges based on any spikes in consumption due to Customer activities.

13. Pre-Requisites

The following pre-requisites must be satisfied before the Services Commencement Date unless otherwise agreed in writing by the Supplier. Failure to satisfy these pre-requisites may delay the commencement of the Service or affect the Supplier's ability to provide the Services. In such circumstances the Supplier shall be entitled to charge the Customer as though the Services had started by the planned Services Commencement Date:

- a. Completion of the Enterprise Pre-Launch Questionnaire (ELQ).
- b. Platform and where applicable WMI access for all monitored services.
- c. Administrative Relevant Access Permissions for all patching and monitored services.
- d. Administrative Relevant Access Permissions for Supplier engineers on supported devices where required.
- e. Registered Microsoft Partner of Record and/or AWS Associated Partner registration.
- f. Administrative access permissions for the Supplier's engineers on supported cloud resource subscriptions/accounts.
- g. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
- h. Run-book delivery & automation requires those specific application or tasks to be on-boarded via the Service Transition Process or Customer Success engagement.
- i. Any devices onboarded for Patching shall be required to meet a minimum standard of N-2.
- j. On-Boarding Health Check and Documentation.
- k. SSH, SNMP and where applicable WMI access for all monitored devices

14. Partner of Record

The Service requires either Cloud Solution Provider (CSP) or Claiming Partner of Record (CPOR) for escalation to Microsoft. Microsoft assigns support rights using data from the CPOR or CSP system therefore, the Supplier must be registered as the Cloud Solution Provider or Claiming Partner of Record on any cloud resource subscriptions that contain or contribute to assets under support or management for the entire duration of the Contract. Consequently, the Customer shall, prior to the Services Commencement Date arrange for the Supplier to be registered as the CPOR or CSP on all cloud resource subscriptions that contain or contribute to assets under support or management for the entire duration of the Contract.

The Customer will grant ANS 24 x 7 operational control and management of a Customer's Azure resources via any of the following options:

- Supplier "Global Administrator" permission within the Customer's Azure active directory tenant.
- Azure Lighthouse delegated resource management.
- Directory of guest users or service principals.

15. Partner Admin Link (PAL)

To ensure the Supplier is recognised by Microsoft as the Partner providing advisory and operational services under this Contract, the Customer shall configure **Partner Admin Link (PAL)** association for all Azure subscriptions that contain or contribute to assets in scope of the Service.

PAL provides Microsoft with visibility of the Supplier's ongoing administrative and engineering activity within the Customer's environment and enables Microsoft to attribute influence, usage, and support context to the Supplier. PAL does not grant any permissions by itself and requires the Customer to assign appropriate Azure RBAC roles to the Supplier's service accounts.

Accordingly, the Customer shall:

- Assign the Supplier the minimum required Azure RBAC role(s) (typically *Contributor* or equivalent) to allow PAL association to be created,
- Maintain this PAL association for the duration of the Contract, and
- Ensure that any newly created or restructured subscriptions are also linked to the Supplier via PAL where those subscriptions contain or contribute to assets under support or management.

This PAL association is required in addition to any Cloud Solution Provider (CSP), Claiming Partner of Record (CPOR), or (where applicable) Transacting Partner of Record (TPOR) registrations outlined in this Service Definition and forms part of Microsoft's mechanisms for recognising the Supplier's involvement in service delivery and escalation.

16. Amazon AWS Associated Partner

Amazon AWS' partnership status is heavily reliant on demonstrating working relationships with AWS consumers. Amazon leverage information collected from the associated partner system to assign partnership status. As such the Supplier must be registered as the associated partner on any accounts that contain or contribute to assets under support or management for the entire duration of the Contract. Consequently, the Customer shall, prior to the Services Commencement Date arrange for the Supplier to be registered as the associated partner on all accounts that contain or contribute to assets under support or management for the entire duration of the Contract.

17. Terms and Definitions

The definitions used in ANS's Terms and Conditions shall have the same meaning when used in this Service Definition. The additional terms used in this Service Definition are defined as follows:

Term	Definition
24 x 7	24 hours a day, 7 days a week.
Additional Service Charges	Charges payable by the Customer for services, activities, or work that fall outside the scope of the contracted Service, are expressly stated in this Service Definition to be chargeable or exceed the included service allowances.
Affected	A User, Site, or system is able to continue operating, in whole or in part, notwithstanding an Incident, whether because the fault is partial, intermittent, or a Workaround is available, as distinguished from "Down."
AI SPM	AI Security Posture Management (AI SPM). A capability within Microsoft Defender for Cloud that assesses the security posture of AI workloads and provides guidance to help identify and reduce security risks.
ANS Glass Portal	The portal where the Customer can log/view Service-related tickets, alerts and performance dashboards.
Annex Document	Sets out the specific terms for any additional services the Customer purchases as stated on the relevant quotation alongside the core Co-Managed Service tier.
Application Code	The Customer owned software code that runs on or interacts with the cloud environment. This includes any scripts, functions, applications, or logic developed or maintained by the Customer and is fully outside the scope of the Supplier's Managed Service.
Assets	Cloud-based resources, subscriptions, or services that are transacted through the Supplier and are within scope of the Service.
Bolt-On Service	An additional service purchased by the Customer alongside the core Co-Managed Cloud Service, with specific terms set out in an Annex Document.
Bug Remediation	The process of identifying, analysing, and resolving defects or errors in an IT service, to restore normal functionality and prevent recurrence.
Business Critical Incident	Incidents that cause complete outage or failure of Service-relevant systems or services identified by the Customer as crucial to normal business operations.

Term	Definition
Change	The addition, modification, or removal of anything that could have a direct or indirect effect on the Service.
Change Advisory	Guidance and recommendations provided by the Supplier in relation to proposed Changes, including assessment of technical approach, impact, risk, and implementation considerations.
Change Advisory Board (CAB) Approval	Change approval of the CAB required as part of the Change Management Process for Normal Changes.
Change Management Process	The Supplier's structured approach to managing Changes.
Change Request	A formal request submitted to the Supplier from the Customer.
Change Request Form	The template that allows the Customer to submit requested Changes via the ANS Glass Portal to the Supplier as part of the Change Management Process.
Code Drift	The divergence between the Customer's desired state (defined in Infrastructure as Code repositories) and the actual, live state of the Customer's environments. This mismatch introduces unpredictable bugs, security vulnerabilities, and deployment failures.
Co-Managed	The Supplier and the Customer share the responsibility of managing the solution. This hybrid approach allows the Customer to remain in control over certain aspects of the solution, while outsourcing more complex or resource intensive tasks to the Supplier.
Co-Managed Cloud Service	The applicable Co-Managed Cloud service purchased by the Customer under this Service Definition, being either the Co-Managed Cloud Advanced Service or the Co-Managed Cloud Premier Service.
Co-Managed Service Tier	The applicable level of the Co-Managed Cloud Service purchased by the Customer, being either Advanced or Premier.
Critical System	Any system, application, or piece of infrastructure identified in this Schedule (or otherwise agreed in writing between the parties) as critical to Customer's core business operations.
Customer	The organisation purchasing and receiving the Managed Service from the Supplier as identified in the quotation.
Customer Success Architecture	Technical capability provided by the Supplier to provide architectural validation and technical expertise.

Term	Definition
Customer Success Reviews	Regular engagement delivered by the Supplier focused on performance and value of the Managed Services contracted.
Demarcation Zone	Infrastructure or solutions are inside the Demarcation Zone if they are Customer Supported Assets. Infrastructure or solutions are outside the Demarcation Zone if they are not Customer Supported Assets.
Down	A User, Site, or system is wholly unable to perform its core function, with no Workaround available, as distinguished from "Affected."
Drift Detection	The process of identifying when the actual state of infrastructure, configuration, or deployed resources differs from the intended state defined in approved code, templates, or configuration baselines.
Emergency Change	A Change required in order to resolve or implement a tactical workaround for a P1 incident.
Enhancement Request	A formal proposal to improve functionality in an existing IT service, system, or process. Submitted when stakeholders identify a desirable change that is not the result of a fault or failure.
Expert Access	The Supplier's provision of specialist technical advice and guidance in response to Customer question or query relating to the relevant Service activity, during the applicable Service Hours.
Feature Requests	A request from a Stakeholder for new functionality or capabilities to be added to an existing IT service or product.
FinOps	Tools and capabilities provided by the Supplier to deliver data driven cloud cost optimisation insights and implementation to the Customer.
Force Majeure	Any event or circumstance beyond a party's reasonable control which prevents or delays that party from performing its obligations under the Contract, including without limitation natural disasters, war, terrorism, industrial action, failure of utilities or communications networks, cyber attack, governmental action, or third-party supplier failure.
GCP	Google Cloud Platform (GCP). The public cloud platform provided by Google.
GitOps	An operational model that applies DevOps principles that supports the management of infrastructure and applications.

Term	Definition
GreenOps	Reporting provided by the Supplier to show available carbon emissions data for applicable cloud resources.
Impact Assessment	Information the Customer is required to provide as part of logging an Incident with the Supplier.
Incident	An unplanned interruption to, degradation of, or reduction in the quality of a service.
Incident Management Process	The Supplier's structured approach to managing Incidents.
Infrastructure as Code (IaC)	The DevOps style approach followed by Supplier in providing Infrastructure as Code services adhering to the clauses stated in the Terms.
Major Incident	An Incident classified by the Supplier as having the highest level of impact and urgency within its internal operations, which deprives multiple customers or businesses of one or more crucial services. This classification relates to a Supplier-wide operational Incident.
Managed Services Handbook	A document provided by the Supplier to provide the Customer with key supporting information regarding their Managed Service provision.
Microsoft Premier Support	Supplier owned support contract with Microsoft.
Monitoring Solution	Tools used by the Supplier to monitor and alert on the health of Customer Supported Assets.
N-2	The version that is two supported releases behind the current release standard. For the purposes of this Service Definition, any device onboarded for patching must be running a version that is no more than two releases behind the then-current supported version.
Normal Business Hours	9:00 -17:30, Monday to Friday (excluding bank holidays in England and Wales)
Normal Change	Change that is not a Standard Change or Emergency Change. It goes through the Change Management Process, including assessment, authorisation and scheduling.

Term	Definition
Priority Level	The classification (P1, P2, P3, P4 or P5) assigned to an Incident in accordance with Section 3 of this Schedule, determining the applicable target Response Time and Resolution Time.
Problem	The underlying cause of one or more Incidents.
Problem Management	The process of identifying and managing the underlying causes of Incidents to prevent recurrence.
Project Change	Change delivered by way of the Supplier's Professional Services.
Pull Request	A request for changes made in source code branch to be reviewed, validated, and approved before being merged into a version-controlled repository.
Response Time	The elapsed time from the logging of an Incident within the ANS Glass portal until the Supplier responds whether via email, the ANS Glass portal update, telephone call or in person.
Resolution	The criteria for resolution are agreed as part of the Impact Assessment. When the criteria is met, the Incident will be marked as resolved and Supplier will contact Customer to confirm the authority to close the Incident.
Resolution Time	The elapsed time, measured in Normal Business Hours unless otherwise stated, from Response Time until the Incident is resolved or a permanent fix is implemented, excluding any period during which Supplier is awaiting information, access, or action from Customer.
Root Cause Analysis	A process used to identify the underlying cause(s) of Incidents or Problems.
Security Incident	An Incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, or security.
Service or Managed Services	A defined set of activities, capabilities, and responsibilities provided by the Supplier to deliver value to the Customer in accordance with the agreed scope, terms, and service levels as set out in this Service Definition.
Services Commencement Date	The date on which the Service starts, as agreed between the Supplier and the Customer.

Term	Definition
Service Desk	The Supplier's central point of contact for logging, managing and resolving Incidents and Service Requests, and for coordinating communications between the Customer and the Supplier in relation to the Managed Service.
Service Hours	The applicable hours for provision of the Service as outlined in the column headed Service Hours in Section 3.
Service Requests	Requests for information, advice, access, or Standard Changes that are not related to failure or degradation of a service.
Service Transition Process	The Supplier's structured approach to the transition of new or changed Services into the Customer's contracted Managed Service.
Sev 'X'	A priority classification from Microsoft Premier Support. Priorities are defined as; A – Critical impact, B – Moderate impact, C – Minimal Impact.
Site	Physical location or office of Customer's (or, where applicable, a distinct logical location such as a data centre or virtual office environment) at which Customer's Users, systems, or infrastructure covered under the Contract are based.
Standard Change	A pre-authorised Change that is low risk and follows a documented process for implementation.
Supplier	ANS Group Limited a limited company incorporated in England and Wales under registration number 03176761 with a registered address at 1 Archway, Birley Fields Manchester M15 5QJ.
Terms & Conditions	The terms and conditions governing the Contract, as identified in the Quotation.
User	An individual authorised by Customer to access or use the services provided by the Supplier under the Contract, including Customer's employees, contractors, and any other individuals the Customer has authorized for that purpose, and, where the context requires, a Department, Site, or system used by such an individual.
Valid Supported Configuration	A configuration of an IT service or component that is formally approved, tested, and supported by the Supplier and Vendor.

Term	Definition
Vendor	A third party who sells or licenses third party services, tools, software or hardware to the Supplier or the Customer (as the case may be) which the Supplier has agreed in writing is within the scope of the Services provided pursuant to this Service Definition.
WMI	Windows Management Instrumentation.
Workaround	A temporary means of avoiding or reducing the impact of an Incident, pending a permanent resolution.
Working Day	8.5 Normal Business Hours