



Service Definition

Co-Managed Security
Advanced & Premier

Contents

1.	Operational Services.....	1
1.1	Service Description.....	1
2.	Service Operations – Advanced and Premier.....	1
3.	ANS Co-Managed Security– Advanced.....	4
3.1	Posture Management.....	4
3.2	Compliance and Governance	5
4.	Optional Bolt-On Services- Advanced Tier	5
5.	ANS Co-Managed Security Service – Premier	7
5.1	Enhanced Cloud, Data & AI Security	7
5.2	Secure Access.....	7
5.3	Agent Governance.....	8
6.	Optional Bolt-On Services- Premier Tier	9
7.	Incident Management	10
7.1	Priority Clarification.....	10
7.2	Impact Assessment Factors	11
7.3	Re-Classification and Escalation	11
7.4	Response SLAs & Target Resolution KPIs Exclusions	12
7.5	Reporting.....	12
8.	Change Management.....	12
8.1	Change Risk Assessment Matrix.....	13
8.2	Change implementation targets Table:	13
9.	Service Levels, Key Performance Indicators and Service Credits.....	14
10.	Exclusions.....	15
11.	Customer Responsibilities	16
12.	Assumptions	18
13.	Pre-Requisites.....	18
14.	Partner of Record	18
15.	Partner Admin Link (PAL)	19
16.	Terms and Definitions	19

1. Operational Services

1.1 Service Description

ANS's Co-Managed Security Service is designed to enable the Customer to strengthen their security posture and get the most out of their security investment. The Supplier delivers this by providing technical expertise, governance, monitoring, and configuration oversight to help reduce risk, maintain secure access, reduce the risk of data leakage, and support compliance requirements.

The Co-Managed approach allows the Customer to remain in control over the strategic direction of their security environment, while outsourcing more complex or resource-intensive security tasks to the Supplier. This makes the Service particularly useful for organisations that want to reduce operational overhead whilst still maintaining visibility, control, and assurance across their security operations.

2. Service Operations – Advanced and Premier

Operations Baseline		
Activities	Service Operations	Service Hours
ANS Glass Portal Access	The Customer will be provided with access to the ANS Glass portal providing visibility of all 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
Incident Management		
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 the Incident Management Process via telephone and remote connection for Priority 1 scenario support 24x7x365. Priority escalation to Microsoft Premier Support is also included at the Premier Tier 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
Change Management & Advisory		
Operational Advisory	The Supplier will provide access to Change Advisory via the Change Management Process for: <ul style="list-style-type: none"> Platform architecture & configuration. Platform optimisation. Security and governance. 	Normal Business Hours
Expert Access	The Supplier will provide access to qualified security professionals for question/query Service Requests.	Normal Business Hours
Change Advisory Board 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 Project Changes.	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 within a two-hour window.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 x 7
Customer Success		
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)	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. Where CoE is purchased by the Customer, items highlighted in the CSR reports can be used to shape CoE backlogs on instruction from the Customer.	Normal Business Hours
Wave Release/Deprecation 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 Security Advanced

3. ANS Co-Managed Security– Advanced

In addition to the above, the Co-Managed Security Service at the Advanced tier (Co-Managed Security Advanced Service) will include the following.

3.1 Posture Management

Posture Management provides Customers with a unified view of their security posture and exposure across their Microsoft security estate. By consolidating insights from across the M365 suite, the service helps customers assess alignment with recognised industry standards, identify areas of risk, and prioritise remediation activities. This enables informed decision-making, supports compliance objectives, and drives continuous improvement of the Customer's security posture.

Activity	Description	Service Hours
Security Framework Insights	The Supplier will provide ad-hoc Microsoft M365 focused Security Framework Assessments, upon request from the Customer. The Supplier will deploy Vendor tooling that enables the Customer to have read-only access to the status of select information around posture policies, compliance and security of the Customer's Microsoft M365 environments through the ANS Glass Portal. Where a more detailed assessment is required, a chargeable engagement will be required.	Normal Business Hours
Identity Management	The Supplier will provide visibility and recommendations around the Customer's Microsoft Entra ID configuration. Upon request, the Supplier will conduct access review reports for users (internal and guests) and groups, as well as identifying risky users and service principles, in line with the Change Management Process.	Normal Business Hours
Device Management	Upon request, the Supplier will provide guidance on how to enrol devices into Microsoft Intune and apply essential compliance settings. Where the Customer requires more detailed guidance or assistance, the Supplier will provide a quotation for a chargeable engagement.	Normal Business Hours
Security Solution Management	The Supplier and the Customer will Co-Manage the security solution provided to the Customer. The Supplier will make recommendations to the Customer on any required actions. The Supplier will provide policy configuration and maintenance of the in scope automated response capabilities, <i>where licensed, supported and onboarded as part of the agreed Service scope</i> . However, ultimate responsibility and approval for configuration will reside with the Customer.	Normal Business Hours
Policy Management	The Supplier will provide a relevant baseline for Microsoft M365 policies in line with a recognised framework such as the CIS as provided by the Supplier's tooling. The Supplier will generate reports on demand highlighting drift from aligned compliance policies. The Supplier will identify causes of drift and recommend corrective actions to restore compliance, in line with the Change Management Process. Where applicable and through the Change Management Process, the Supplier will assist in the generation of policy impact analysis, to help the Customer understand the impact of aligning individual policies as provided by the Supplier's tooling.	Normal Business Hours

3.2 Compliance and Governance

Compliance and Governance aims to safeguard organisational data and systems against unauthorised access, misuse, and threats. This element of the Service includes implementing security controls, and aligning compliance with relevant standards to maintain confidentiality, integrity, and availability.

Activity	Description	Service Hours
Information Security	In Context of Microsoft 365, the Supplier will conduct reviews on an agreed cadence of the Customer's information security baseline. The Supplier will report back to the Customer any insights, anomalies and recommendations. Upon request and following the Change Management Process, the Supplier will make modifications to Customer Supported Assets configuration. The Supplier will act strictly on Customer instructions for configuration. The Supplier will not define the information security strategy on behalf of the Customer.	Normal Business Hours
Information Compliance	In Context of Microsoft 365, the Supplier will conduct reviews on an agreed cadence of the Customer's information compliance baseline. The Supplier will report back to the Customer any insights, anomalies and recommendations. Upon request and following the Change Management Process, the Supplier will make modifications to Customer Supported Assets configuration. The Supplier will act strictly on Customer instructions for configuration. The Supplier will not define the information compliance strategy on behalf of the Customer.	Normal Business Hours
Information Governance	The Supplier will conduct reviews on an agreed cadence and make recommendations to the Customer in relation to SharePoint Online and OneDrive governance from within SharePoint Advanced Management. The Supplier will highlight any areas that should be investigated further by the Customer such as content sprawl, managing content lifecycle and streamlining permission/access management.	Normal Business Hours

4. Optional Bolt-On Services- Advanced Tier

The Customer has the option to consume additional Services to the Co-Managed Security Service Advanced tier 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 Security Service Advanced tier, the specific terms, activities, exclusions, responsibilities, assumptions, and pre-requisites relating to the Bolt-On Service will be outlined in an Annex Document. These are in addition to the terms outlined in this document.

Applicable Bolt-On Services are available here: [Service Definitions](#) | [ANS Service Definitions](#)

Co-Managed Security Premier

5. ANS Co-Managed Security Service – Premier

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

5.1 Enhanced Cloud, Data & AI Security

Microsoft Defender for Cloud combines multiple cloud security tools to protect applications across their entire lifecycle. It extends protection to Azure components such as Azure App Service, containers, application programming interfaces (APIs), Key Vault, storage, databases, internet of things (IoT), CSPM (Cloud Security Posture Management) and EASM (External Attack Surface Management).

Activity	Description	Service Hours
Cloud Platform Compliance	The Supplier will conduct reviews on an agreed cadence of the Customer's Azure Cloud platform compliance posture which optionally includes additional Azure components identified and onboarded as Customer Supported Assets. Following the review, the Supplier will report back to the Customer any insights, anomalies and recommendations that can be actioned in line with the Change Management Process.	Normal business Hours
Cloud Platform Compliance Configuration	Upon request and following the Change Management Process, the Supplier will make modifications to the Customer's compliance posture. The Supplier will act on Customer instruction for configuration of the above areas. The Supplier will not define the compliance strategy on behalf of the Customer.	Normal business Hours

5.2 Secure Access

Secure Access is designed to provide monitoring, policy management, guidance, and operational support to help customers run their Microsoft Global Secure Access environment securely and effectively. Customers will get access to specialist support to maintain platform health, manage GSA-aligned access policies, support internet and private access configurations, and provide ongoing review and advisory services to help keep the service aligned to agreed standards and evolving business requirements.

Activity	Description	Service Hours
Platform Monitoring	<p>The Supplier will monitor the health and availability of Microsoft Global Secure Access service components and connectors within the Customer tenant, including internet access and private access services where enabled.</p> <p>Upon an agreed cadence, the Supplier will review and provide recommendations around the Customer's Microsoft Global Secure Access configuration, including reporting on service activity, and posture reviews to identify risks and improvement opportunities within agreed service boundaries.</p>	<p>24 x 7 (monitoring) Normal Business Hours (response)</p>

Conditional Access Policy Management	The Supplier will manage Conditional Access Policies used to enforce Global Secure Access, including internet access and private access controls, in line with the agreed Change Management Process.	Normal Business Hours
Baseline Policy Management	The Supplier will provide recommendations on an ad hoc basis and drift management of relevant Global Secure Access Conditional Access Policies, aligned to Supplier best-practice frameworks.	Normal Business Hours
Security Profile Management	Upon request, the Supplier will manage and maintain Microsoft Global Secure Access (GSA) internet and private access in line with agreed service boundaries and Change Management policies.	Normal Business Hours
Alert Escalation	Where the Customer also has Supplier SOC Services, Global Secure Access may be integrated into the Supplier SOC workflows in line with an agreed scope, as part of Additional Service Charges.	24 x7

5.3 Agent Governance

Agent Governance supports the Customer in governing and securing AI agents across their environment. The Supplier provides visibility, insights, and recommendations to help the Customer manage agent identity, access, lifecycle, and risk posture using Microsoft security and governance tooling.

Activity	Description	Service Hours
Agent Lifecycle Management	<p>The Supplier will periodically review the agent inventory to identify unregistered or unmanaged agents and provide recommendations to bring them under agreed governance in line with the Change Management process.</p> <p>Upon request, the Supplier will provide advisory oversight for the onboarding of new AI agents and material changes to existing agents, ensuring identity, access, and governance controls are applied in line with Customer policies and the Change Management Process.</p>	Normal Business Hours
Agent Risk Monitoring	The Supplier will periodically review and provide recommendation around agent risk posture, identifying items such as high-risk agents, anomalous behaviour, and policy violations.	Normal Business Hours
Agent Compliance	Upon request, the Supplier will provide recommendations and reporting aligned to audit, data protection, and AI governance requirements using Microsoft Purview and Agent 365 signals, supporting Customer audit readiness.	Normal Business Hours

6. Optional Bolt-On Services- Premier Tier

The Customer has the option to consume additional Services to the Co-Managed Security Service Premier Tier 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 Security Service Premier Tier, the specific terms, activities, exclusions, responsibilities, assumptions, and pre-requisites relating to the Bolt-On Service will be outlined in an Annex Document. These are in addition to the terms outlined in this document.

Service Definitions for optional Bolt-On Services can be found 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 the 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 the 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 ANS ITSM Tool
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 – 24x7 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 Base Charge and in any event, shall not exceed 10% of the monthly Base 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 or the Customer Supported Assets within the scope of Service resulting in impact to the Service.
- Issues resulting from unauthorised access by the Customer outside of the scope of Service.
- The provision of 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, AWS or Google).
- 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 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.
- 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.
- Any works relating to the technical operation, uptime, application metrics, resilience & failover of the cloud environment is out of scope of the Co-Managed Security Service.
- The Supplier can only provide support for features that are in General Availability.
- The Customer's technology failing to respond to an execution command initiated by the Supplier to a containment activity.
- Issues created by the Customer on systems that affect the scope of Service that impact the ability for the Supplier to deliver the Service.
- The Supplier does not provide vendor integrated Digital Forensic Incident Response retainer services.
- The Supplier will not include Digital Forensic Analysis where the Incident Management Process is provided.

- p. The Service is not an IT operational monitoring service or problem identification service, and the Supplier is not responsible for IT operational under-performance or issue identification.
- q. The Services are provided remotely and if the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.
- r. The Supplier will not proceed without Customer authorisation where additional costs are to be raised. The Customer will hold all liabilities in the event that such authorisation is not given.
- s. Detection engineering, tuning, and ongoing optimisation of third-party alert sources are excluded unless expressly agreed in the Quotation or as otherwise agreed in writing.
- t. For the avoidance of doubt, the Co-Managed Security Service does not include continuous security alert triage, threat investigation or cyber incident response unless expressly included within the Customer's Quotation or provided under a separately contracted SOC or MDR service.

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.
- 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 licenced 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 completing a Change Request in accordance with the Supplier's Change Management Process.
- i. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook.
- j. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier).

- k. 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.
- l. 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.
- m. 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.
- n. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.
- o. It should be noted that 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 onboard the Service.
- q. Provide the Supplier with technical access and relevant permissions to deliver the Service, including providing the Supplier with authorisation and technical access to enable automated response for containment.
- r. Attend any Service orientation calls at the start of delivery of the Service, providing required information to support the successful implementation of the technical infrastructure;
- s. Assist the Supplier in the remediation of issues that may prevent operation of the Service;
- t. Advise the Supplier two (2) Working Days in advance of any penetration testing or additional vulnerability scanning so that the Supplier can apply the relevant context to the alerts.
- u. 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;
- v. Attend meetings scheduled at mutually convenient times;
- w. Inform the Supplier, with a minimum of 5 Working Days' notice, of any relevant change that may impact the operation of the Service;
- x. Provide out of hours contact details for nominated individuals in order to be notified of any relevant Security Incident and provide Customer representation on Incidents;
- y. Update the Supplier of changes to nominated individuals on the Customer account and associated contact details;
- z. Support the Supplier with timely decision making in order to enable the appropriate countermeasures to a Security Incident to be deployed or enacted;
- aa. Apply all reasonable remediation recommendations to the Customer Supported Assets or the in scope Customer's environment. Where this is not implemented by the Customer within a reasonable time, the Supplier may increase the Charges to accommodate for additional time and effort to detect and remediate recurring Security Events and Incidents. The Supplier's Standard Published Rates will apply;
- bb. Acknowledge and respond to Incidents escalated by the Supplier with individuals nominated by the Customer to be included in the Security Event notification process;
- cc. Provide reasonable availability of Customer representative(s) when resolving a Security Incident or Service Request.
- dd. Pre-authorise the Supplier to make changes to the detection ruleset and policies without a Change Request or written Customer agreement. The Supplier will always act in good faith in implementing or tuning the rules to provide the best prevention, detection and response services to the Customer;
- ee. Acknowledge that any changes by the Customer which disrupt the Service will be subject to Additional Service Charges, at the Supplier's Standard Published Rates, to rectify and remediate;
- ff. The Supplier will not proceed without the Customer's authorisation where Additional Service Charges are applicable. The Customer shall be liable for any and all consequences where it does not provide such authorisation where required to deliver the Services; and
- gg. The Customer acknowledges that this is a co-managed service, with the Supplier supporting the Customer in its management of its security. The Supplier shall not be liable for Security Incidents or other consequences arising from the Customer's security arrangements whether in relation to these Services or otherwise.

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 SLA, and/or any Charges:

- a. All Customer Supported Assets and production AWS and Azure accounts (as relevant) within the Demarcation Zone under the Contract are covered by a valid software maintenance and support agreement in line with applicable SLA.
- b. All Customer Supported Assets are in a Valid Supported Configuration at the Commencement Date.
- c. All Customer specific pre-requisites have been completed before the 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 onboard the Service.
- f. The Supplier reserves the right to restrict utilisation of the Customer Success Architect capability to 10 hours per calendar month.
- g. 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.
- h. The Supplier will refer any actions or activities required that are outside of the scope of the Service to the Customer with options for consideration and decision making. This may involve additional project work or Professional Services and Additional Service Charges.
- i. Customer approves the use of Microsoft Defender automated investigation and response capabilities, acknowledging potential temporary service impact.

13. Pre-Requisites

The following pre-requisites must be satisfied before the 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. On-boarding health check and documentation.
- b. Platform, Microsoft Defender and, where applicable, WMI administration permissions and access and configuration for all performance monitored and in scope Services.
- c. Supplier being registered as the Microsoft Partner of Record and/or AWS Associated Partner registration.
- d. Granting of administrative access permissions for the Supplier's engineers on supported Cloud Resource Subscriptions/accounts.
- e. Run-book delivery & automation requires those specific application or tasks to be on-boarded via the Service Transition Process or Customer Success engagement.

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 the 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, Claiming Partner of Record, 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. Terms and Definitions

The definitions used in ANS' Terms & 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.

Term	Definition
Advanced	The advanced tier of the Service, as described in this Service Definition.
Advice	Guidance or recommendations provided by the Supplier about the Service provided using reasonable care and skill to be expected of a reasonably competent supplier of managed IT and cyber security services.
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.
ANS Glass Portal	The portal where the Customer can log/view Service-related tickets, alerts and performance dashboards.
Bolt-On Service	An additional Service purchased by the Customer alongside the core Co-Managed Security 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.
Centre of Excellence (CoE) Service	The Supplier's delivery model that provides access to a wide range of skills and experience across the technology sectors that ANS specialises in. This service enables customers to innovate, accelerate digital transformation, and ensure the continuous evolution of their business and its technology.
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 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.

Term	Definition
CIS Standards	Security configuration benchmarks and best-practice guidance published by the Centre for Internet Security (CIS), used as a reference framework to assess and advise on security posture and configuration alignment.
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 Security Service	The Service described in this Service Definition.
Compliance Score	Microsoft's measurement of the Customer's compliance posture, based on completed improvement actions, assessments, and related controls in the applicable Microsoft compliance tools.
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 expertise.
Customer Success Review	Regular engagement delivered by the Supplier focused on performance and value of the Managed Services contracted.
Data Security Posture Management (DSPM)	Capabilities within Microsoft security tooling that provide visibility, insights, and recommendations relating to the security posture, sensitivity, and risk exposure of organisational data.
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.
Digital Forensic Analysis	The examination of digital evidence to investigate Security Incidents.
Emergency Change	A Change required to resolve or implement a tactical workaround for a P1 Incident.
Enhancement Requests	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.

Term	Definition
Feature Requests	A request from a stakeholder for new functionality or capabilities to be added to an existing IT service or product.
General Availability	The status of a product, feature, or service when it is fully released for production use and supported by the third-party provider.
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.
Incident Response	Actions taken to investigate, contain, and mitigate a suspected or confirmed Security Incident.
IT Service Management (ITSM) Tool	The Supplier's service management system used to log, track, manage, and report on Incidents, Service Requests, Changes, and related service activities.
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 the Managed Service provision.
Microsoft Premier Support	Supplier owned support contract with Microsoft.
Normal Business Hours	9:00 -17:30, Monday to Friday (excluding bank holidays in England and Wales)
Normal Changes	Change that is not a Standard Change or Emergency Change. It goes through the Change Management Process, including assessment, authorisation and scheduling.

Term	Definition
Premier Tier	The premier tier of the Service, as described in this Service Definition.
Priority	The scale and severity of an Incident, including P1-P5, as expressed in the Incident Priority Table below.
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.
Response	Is the action taken by the Supplier to acknowledge alert/s and begin an investigation into the status of the alert/s.
Root Cause Analysis	A process used to identify the underlying cause(s) of Incidents or Problems.
Security Framework Assessments	Assessment of the Customer's security posture against recognised security frameworks and standards, used to identify gaps, provide recommendations, and support improvement planning.
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.
Security Platform	The security tooling environment used by the Customer and/or the Supplier to support security monitoring, alert correlation, case management, investigation, orchestration, and response activities in connection with the Service.
Security Orchestration, Automation and Response (SOAR)	Capabilities used to orchestrate, automate, and support security investigation and response activities.

Term	Definition
Security Operations Centre (SOC)	A centralised operational function operated by the Supplier that provides security monitoring, alert triage, investigation, and response activities using security tooling and defined operational processes, in accordance with the scope of the contracted Service.
Service or Managed Service	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.
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 Transition Process	The Supplier's structured approach to the transition of new or changed services into the Customer's contracted Managed Service.
Service Requests	Requests for Information, Advice, access, or Standard Changes that are not related to failure or degradation of a Service.
Sev 'X'	A priority classification from Microsoft Premier Support. Priorities are defined as: A – critical impact; B - moderate impact; C – minimal impact.
SharePoint Advanced Management	A Microsoft capability that helps organisations strengthen governance, security, and lifecycle management across SharePoint Online and OneDrive.
Standard Change	A pre-authorised Change that is low risk and follows a documented process for implementation.
Standard Published Rates	The Supplier's standard published charges for services or work not included within the contracted Service.
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.

Term	Definition
Terms & Conditions	The terms and conditions governing the Contract, as identified in the Quotation.
Valid Supported Configuration	A configuration of an IT service or component that is formally approved, tested, and supported by the Supplier and Vendor.
Well Architected Framework	A set of best practices and principles designed to help architect secure, high-performing, resilient, and efficient infrastructure.
WMI	Windows Management Instrumentation.
Working Day	8.5 Normal Business Hours.