Service Definition

Co-Managed Security

Contents

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

1. Operational Services

1.1. Service Description

The Co-Managed Security Service provides governance, monitoring and configuration oversight to help prevent data leakage, maintain secure access, and support compliance requirements. The Supplier delivers the required tooling and security expertise while allowing the Customer to retain control of their environment and strategic direction.

The Service provides:

- Efficient use of Microsoft security capabilities to support the Customer's existing investment.
- Visibility of governance, posture and configuration through defined reporting and insights.
- Reduced operational effort for the Customer by transferring agreed security management activities to the Supplier.

1.2. Service Tiers

Tiers	Services Included	Optional Bolt-on Service
Standard	• Security Framework Assessments • Posture & Exposure Insights • Policy Drift Management • Information security & Compliance	• Endpoint Detection and Response (EDR) • Extended Detection and Response (XDR) • SOC Services
Premier	• Enterprise MDR	• Centre of Excellence (CoE)*

*Minimum committed CoE hour contract

Service Definitions for all optional bolt-on services can be found here: Service Definitions | ANS Service Definitions

1.3. Terms and Definitions

The definitions used in the Terms 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
Normal Business Hours	9:00 -17:30, Monday to Friday (excluding bank holidays in England and Wales)
Working Day	8.5 Normal Business Hours
24 x 7	24 hours a day, 7 days a week
Annex Document	sets out the terms for any additional services the Customer purchases as stated on the relevant Quotation alongside the core Co-Managed Service Tier applicable to the Customer as stated on the relevant Quotation. The terms are additional to those applicable to the relevant Co-Managed Service Tier.
ANS Glass	the portal where the Customer can log/view Service-related tickets, alerts and performance dashboards.
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 systems or services identified by the Customer as crucial to normal business operations.
CAB Approval	change approval of the CAB required as part of the Change Management Process for Normal Changes.
Change	the addition, modification, or removal of anything that could have a direct or indirect effect on the Service.
Change Management Process	the Supplier's structured approach to managing Changes.
Change Request Form	template that allows the Customer to submit requested Changes to the Supplier as part of the Change Management Process.
Customer Success Engineering	technical resource provided by the Supplier to provide architectural validation and technical expertise.
Customer Success Manager (CSM)	non-technical resource provided by the Supplier to facilitate delivery of value to the Customer as part of the Managed Service.

Customer Success Review	regular meeting delivered by the Supplier focused on performance and value of the Managed Services contracted.
Customer Supported Assets	The specific customer owned systems, resources, configurations, or service components that have been formally onboarded into the managed service, meet all prerequisite conditions, and fall within the Supplier's agreed scope for support, monitoring, incident management, and change management. These assets must be in a valid supported configuration, carry appropriate licensing and vendor support, and be accessible to the Supplier with the necessary administrative permissions to deliver the service. Only assets meeting these conditions are treated as "supported," with all other customer assets considered outside the service scope.
Demarcation Zone	infrastructure or solutions not being Customer Supported Assets.
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 or add new functionality to an existing IT service, system, or process. Submitted when stakeholders identify a desirable change that is not the result of a fault or failure.
Feature Requests	a request from a stakeholder for new functionality or capabilities to be added to an existing IT service or product.
Impact Assessment	information the Customer is required to provide as part of logging an Incident with the Supplier.
Incident Management Process	the Supplier's structured approach to managing Incidents.
Major Incident	Incidents categorised as P1 using the incident priority table in this document.
Managed Services Handbook	document provided by the Supplier to provide the Customer with key supporting information regarding Managed Service provision.
Microsoft Premier Support	Supplier owned support contract with Microsoft.

Normal Changes	Change that is not a Standard or Emergency Change. It goes through the Change Management Process, including assessment, authorisation and scheduling.
Project Change	Change delivered by way of the Supplier's Professional Services.
Root Cause Analysis	A process used to identify the underlying cause(s) of Incidents or problems.
Service Disruption Report	Incident report completed by the Supplier.
Service Hours	the applicable hours for provision of the Service as outlined in the column headed Service Hours below.
Standard Change	a pre-authorised Change that is low risk and follows a documented process for implementation
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 Transition Process	the Supplier's structured approach to the transition of new or changed services into the Customer's contracted Managed Service.
Sev B	a priority classification from Microsoft Premier Support. Priorities are defined as; A – Critical impact, B – Moderate impact, C – Minimal Impact
Valid Supported Configuration	a configuration of an IT service or component that is formally approved, tested, and supported by the organisation 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.

1.4. Service Operations

Operations Baseline		
Activities	**Service Operations**	**Service Hours**
Glass Portal Access	Customer access to 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. Problems are reviewed during the Service Management Review.	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 incident management via ANS Glass, Telephone, Teams, Email, 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 Premier support is also included at the Premier Tier.	24 x 7
	Change Management & Advisory	
Operational Advisory	The Supplier provides access to Change advisory for: • Platform architecture & configuration. • Platform Optimisation. • Security and Governance.	Normal Business Hours
Expert Access	The Supplier provides access to qualified Security Professionals for question/query Requests.	Normal Business Hours
Change Advisory Board Authority	The Supplier will act as Change Advisory Board Authority for all Changes considered Standard Changes or Normal Changes for the Customer Supported Assets. 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 access to a Customer Success team to provide architectural validation and technical expertise, working with the customer to understand their long-term goals.	Normal Business Hours
Customer Success Manager	The Supplier will provide a Customer Success Manager to facilitate delivery of value to the Customer as part of the Managed Service.	Normal Business Hours

Wave Release/Deprecations Awareness	The Supplier will make the customers aware of any relevant new/deprecated features in a timely manner.	Normal Business Hours

Co-managed Security Standard

Security Framework Assessments | Posture & Exposure Insights | Policy Drift Management | Information Security & Compliance

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

Issue No: 1.0 Issue Date: 21/01/2026 Classified: Public

2. ANS Co-Managed Security– Standard

For organisations who need to manage sensitive data without additional operational overhead, our Co-Managed Security Standard Service offers:

- Best in class information security, agent creation and sponsorship policies that protect against accidental data leakage.
- Advice on compliance to meet regulatory demands
- Visibility into data across the customer's organisation to support strategic decisions
- Continuous monitoring of interactions with sensitive data
- Access to Purview and Entra's native reporting to simplify audit preparation and prove compliance.

2.1. Security Framework Assessments

Activity	Description	Service Hours
M365 management and security Portal Access	The Supplier will deploy 3rd Party tooling that enables the Customer to have read-only access to a portal providing visibility for the status of posture policies, compliance and security of the Customers M365 environments.	24 x 7
Security Framework Assessments	The Supplier will provide ad-hoc M365 focused Security Framework Assessments, in line with CIS standards, upon request from the Customer. The scope of the assessment falls in line with The Suppliers automated tooling. Where a more detailed assessment is required, a chargeable engagement will be required.	Normal Business Hours

2.2. Posture and Exposure Insights

Posture and Exposure insights focuses on managing user identities and controlling access to resources. It covers processes for authentication, authorisation, and enforcing security policies to ensure only the right individuals have appropriate access to systems and data.

Activity	Description	Service Hours
Entra ID Insights	The Supplier will provide visibility and recommendations around The Customers Entra ID configuration encompassing the following areas • Identity Secure Score • Compliance Issues • Security Risks • Configuration Issues • User Activity Status • High Level Licensing problems	24 x 7
Entra Access, Risk and Analytics Reports	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 Change Management processes. The supplier will provide best practice advice and guidance around sign-in trends, failed logins and Entra activity.	Normal Business Hours
Intune Device Advisory	Upon request, the supplier will provide guidance on how to enrol devices into 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

2.3. Policy Drift Management

Policy Advisory provides guidance on creating, reviewing, and maintaining security policies to ensure compliance with organisational standards and regulatory requirements. It focuses on advising best practices for policy alignment, risk reduction, and consistent enforcement across the environment.

Activity	Description	Service Hours
M365 Baseline Policy Advisory	The Supplier will provide comprehensive baseline M365 policies in line with recognised frameworks such as the Centre for Internet Security (CIS). The Supplier will provide insights into where The Customers policies deviate from the recommended baseline and provide recommendations on how to bring the policies into alignment, in line with Change Management processes. Where significant effort is required, a chargeable engagement may be required to achieve full alignment. Areas covered by the policy baselines include: • Entra	Normal Business Hours

	• Intune • Teams • SharePoint • M365 Admin Centre • Purview	
Policy Drift Reporting	The supplier will generate reports highlighting drift from aligned compliance policies. The Supplier will identify root causes of drift and recommend corrective actions to restore compliance, in line with Change Management processes. Where appropriate the Supplier will assist in the generation of Policy Impact analysis, to help The Customer understand the impact of aligning individual policies.	Normal Business Hours
Daily incremental Backup	The Supplier will perform daily backups of The Customers in-scope Microsoft 365 policies with monthly retention, via automated tooling.	Normal Business Hours
Policy Restore	The Supplier will restore the required in-scope Microsoft 365 policies upon request, in line with Change Management Processes. The Supplier will attempt to recover the affected policies on a best endeavour basis but cannot guarantee successful rollbacks.	Normal Business Hours

2.4. Information Security and Compliance

Information Security safeguards organisational data and systems against unauthorised access, misuse, and threats. This element of the service includes implementing security controls, monitoring for vulnerabilities, and ensuring compliance with relevant standards to maintain confidentiality, integrity, and availability.

Activity	Description	Service Hours
Compliance Reviews	The Supplier will conduct reviews on an agreed cadence of The Customers compliance posture, examples of the areas for review include: • Execute and review pre-defined audit searches. • Review of Compliance alerts based on Customer-defined configurations. • Review Communication compliance for Microsoft recommended actions, policy health, and overall security posture. • Review Compliance Score, improvement actions, and assessments. • Review Communication Compliance, DLP, Information Protection and Insider Risk, including configurations, labels, and behaviours.	Normal Business Hours

	• Review Microsoft 365 Copilot and AI usage. • Review Purview Data Risk Assessments. Following the review, The Supplier will report back to the customer any insights, anomalies and recommendations that can be actioned in line with Change management processes.	
Compliance Configuration	Upon request and following Change Management processes, the Supplier will make modifications to The Customers compliance posture. Examples of areas for modification include: • Create e-discovery cases and searches with the parameters provided by The Customer. • Create and modify retention labels, sensitivity labels, classifiers, and policies. • Configure or modify Information Barrier segments, DLP policies, DSPM and Risk policies. • Mark improvement actions as completed or ignored based on evidence provided by The Customer. The Supplier will act strictly on Customer instructions for configuration of the above areas. The Supplier will not define the compliance strategy on behalf of The Customer but will provide guidance and Advice.	Normal Business Hours
SharePoint online Review and 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

3. Optional Bolt-On Services- Standard Tier

The Customer has the option to consume additional Services to the Security Standard 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 Standard 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 additive to the Terms outlined in this document.

Bolt-On Services applicable at the Standard Tier are;

- Defender Extended Detection & Response
- SOC Services

Service Definitions for all optional bolt-on services can be found here: [Service Definitions | ANS Service Definitions]

Co-managed Security - Premier

Enterprise MDR

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

Issue No: 1.0 Issue Date: 21/01/2026 Classified: Public

4. ANS Co-Managed Security Service – Premier

Premier level Service tier is inclusive or the Core capabilities within the Standard Level and;

4.1. Enterprise MDR

The Supplier's Managed Detection and Response (MDR) Service is designed to provide the right level of response to meet the Customer's needs, ultimately better securing their business. The service is delivered through a partnership defined by the Supplier to meet the cyber security needs of the Customer.

Enterprise MDR is underpinned by ANS SOC Services and as such the Customer will receive all the value of that Service.

A summary of the Service is as follows:

- provision of a Security Operations Centre (SOC) facility with operational resilience for business continuity 24/7.
- trained Security Analysts and Engineers.
- detection rule and process management.
- alert triage and assessment with threat intelligence.
- security analysis with customer business contextualisation.
- threat Detection and Response.
- Incident Response and Containment.
- Security Incident Management, with appropriate advice and guidance.
- Telephone and email support.
- Early value realisation through Supplier accelerated onboarding.

Activity	Enterprise MDR	Service Hours
Security Product Deployment & Management	The Supplier will deploy (where applicable) and manage the Customer's Microsoft Security products as defined in the Scope of Services.	Normal Business Hours
Security Configuration & Correlation	The Supplier will configure relevant correlation rules, apply security-related asset tagging, and implement appropriate security settings	Normal Business Hours
Alert Management & System Tuning	The Supplier will manage alert signals and proactively tune the system to reduce false positives	Normal Business Hours
Data Flow Optimisation	The Supplier will manage data flow into the environment to enable cost efficiency and reduce tool operation costs.	Normal Business Hours
Platform Monitoring	The Supplier will monitor the named Microsoft security platform for operational performance and availability.	24 x 7
Security Tooling Management	The Supplier will provide management of the security tooling during normal business hours	24 x 7

Access Control Management	The Supplier will provide and manage access control for all Supplier staff required to deliver the service.	24 x 7
Security-Vetted Staffing	The Supplier will provide security-vetted staff that meet the Customer's security requirements, at the Customer's expense. Where Government-level vetting is required, the Customer will sponsor all relevant Supplier staff.	24 x 7
UK-Based SOC Provision	The Supplier will provide a Security Operations Centre (SOC) facility with Supplier staff based in the United Kingdom.	24 x 7
Service Reviews	The Supplier will conduct service reviews at a regular cadence to discuss service quality and address any issues.	Normal Business Hours
Monthly Service Reporting	The Supplier will produce monthly reporting in the form of a dashboard displaying relevant events resulting from service delivery.	Normal Business Hours
Activity	**Managed Threat Detection & Response**	**Service Hours**
Detection Rule Development & Management	The Supplier will develop detection rules and other capabilities and manage them as part of the service.	24 x 7
Alert Investigation & Triage	The Supplier will provide investigation and triage on all alerts using skilled security analysts and apply unique Customer context.	24 x 7
Alert Status Assessment	The Supplier will analyse each alert and assess its status in relation to positivity (True-Positive or False-Positive).	24 x 7
Threat Intelligence Integration	The Supplier will use Threat Intelligence information from various sources as part of alert analysis and event enrichment.	24 x 7
False-Positive Handling	The Supplier will close alerts identified as false and refer them for tuning analysis where applicable.	24 x 7
True-Positive Incident Creation	The Supplier will raise a security incident and associated service ticket in the ITSM tool where the alert is a true-positive.	24 x 7
Security Event Investigation	The Supplier will investigate the security events generating the alerts to determine the nature and status of the events.	24 x 7
Incident Response Initiation	The Supplier will create a security incident and commence Incident Response procedures where the security event is malicious or potentially harmful.	24 x 7
MITRE ATT&CK Classification	The Supplier will provide classification using the MITRE ATT&CK framework to categorise various activities. Classification will be	24 x 7

	automatic and set against Microsoft security tooling and the Supplier's chosen security platform.	
Security notification	The Supplier will provide security notification 24/7.	24 x 7
Activity	**Incident Response**	**Service Hours**
Third-Party Alert-Based Response	The Supplier will provide an Incident Response based on alerts generated by the Customer's existing third-party security providers and use the third parties automated technical tooling analysis and collection to respond to suspicious security events detected within the Customer IT infrastructure.	24 x 7
Security Event Investigation & Remediation	The Supplier will investigate the security events generating the alerts, analyse the data, and provide a security response through appropriate containment, eradication, and recovery strategies applicable to the event. The response will include remediation guidance to the Customer and operational support to the Supplier's resolver teams.	24 x 7
Industry-Standard Containment & Eradication	The Supplier will provide containment and eradication responses to detected threats following recognised industry models (NIST, NSCS, SANS).	24 x 7
Immediate Containment Actions	The Supplier will initiate containment actions at the first indication of suspected or actual malicious behaviour and must be enabled to do this using the Customer's tooling.	24 x 7
Root Cause Support	The Supplier will provide a response that supports basic root cause investigation.	24 x 7
Timely Containment Delivery	The Supplier will undertake all reasonable endeavours to deliver a containment response in a timely manner.	24 x 7
Priority Incident Management	The Supplier will manage incidents where a P1 Incident has been declared; this will be downgraded to a P2 Incident once a successful containment response has been applied.	24 x 7
Activity	**Incident Management**	**Service Hours**
Incident Management & Coordination	The Supplier will provide a service that covers Incident Management activities and helps coordinate the relevant resolver groups to remediate the security event or issue in line with the current contracted services.	24 x 7
Security Alert & Incident Response	The Supplier will initiate response to detected Security Alerts and Incidents, as defined within the Supplier Schedule Two (Service Levels).	24 x 7

Priority 1 Incident Reporting	The Supplier will provide Priority 1 Security Incident reporting post a Security Incident and, within ten (10) working days, produce a basic report detailing the timeline of the Incident along with any known root cause and preventative measures.	24 x 7
ITSM Process Adherence	The Supplier will provide adherence to standard contracted Supplier processes for Service Request, Incident, Change and Problem Management underpinned by the Supplier's IT Service Management tooling.	24 x 7
Emergency Change Guidance	The Supplier will provide Emergency Change guidance as required to remediate Cyber Security Incidents and, in the event of a significant and/or destructive Cyber Security Incident, may apply a short-term containment action before formal Customer approval is received. The Supplier will act in good faith and the Customer will not hold the Supplier liable for any of these actions or variable outcomes.	24 x 7
Incident Communication	The Supplier will provide Cyber Security Incident communication throughout Incidents. The frequency of communication may vary depending on the severity of the Incident.	24 x 7
Conference & Bridging Support	The Supplier will provide bridging/conference capabilities using Supplier-provided tools and establish calls where multiple parties (including third parties) are required to support the remediation of an Incident.	24 x 7
Out-of-Scope Referral	The Supplier will refer any actions or activities required that are outside of the contracted services to the Customer with options for consideration and decision-making. This may involve additional project work or Professional Services at additional cost.	Normal Business Hours
Incident Process Initiation & Management	The Supplier will provide Security Incident process initiation and management, adhering to the Supplier's standard Cyber Security Incident Management processes. This includes investigation, assessment, communication, containment and mitigation advice to resolve and/or prevent threats and attacks (subject to scope of the Managed Services provided; otherwise, Professional Services may be available at an additional charge).	24 x 7
Eradication & Remediation Support	The Supplier will provide support to eradication and/or remediation actions and activities required to resolve security incidents within scope of the MDR Service and wider Customer contracted service for support. Any support required outside of	24 x 7

	the contracted services (design change or unsupported infrastructure) will be referred to the Customer with options for consideration. This may involve additional project work or Professional Services at additional cost to the Customer.	
Activity	**Threat Hunting**	**Service Hours**
Proactive Threat Hunting	The Supplier will provide a service that proactively searches for indications of malicious activities not identified by the security tooling.	Normal Business Hours
Data Source Utilisation	The Supplier will use data collected by the security tooling as the source for searches. Devices and Information Systems not covered by the Customer's security tooling are excluded from threat hunt searches.	Normal Business Hours
Sentinel-Based Threat Hunting	The Supplier will conduct Threat Hunting within the Customer's provision of Microsoft Sentinel SIEM, and the Customer will maintain a valid licence with a minimum of 90 days of searchable content.	Normal Business Hours
IoC-Driven Searches	The Supplier will use identified Indicators of Compromise (IoC) from various Threat Intelligence providers as the primary basis for searches. This will include known threat actor groups and their associated techniques, tactics, and procedures (TTPs).	Normal Business Hours
Industry Threat Hunting	The supplier will conduct threat hunts on threats identified against the Customers Industry, identified Advanced Persistent Threats (ATP) targeting the UK, relevant TTPs that are in use against UK organisations.	Normal Business Hours
Monthly reporting	The supplier will conduct threat hunts on a monthly basis and provide a report to the Customer on the search scope and findings.	Normal Business Hours
Trained Security Analysts	The supplier will provide trained security analysts to undertake the Threat Hunting.	Normal Business Hours
Activity	**Supplier Security Platform**	**Service Hours**
Security Orchestration, Automation and Response (SOAR) capabilities	The supplier will provide its own Security Orchestration, Automation and Response (SOAR) capabilities. The technology used will be at the Supplier's discretion for best service.	24 x 7
Identified Data Feeds	The supplier will take identified data feeds from Customer tooling to enrich and manage through the Supplier defined processes.	24 x 7

Augmented Threat Intelligence	The supplier will apply additional Threat Intelligence augmentation to alert and events in the Suppliers Security platform for analysis in the platform.	Normal Business Hours
Correlate Events	The supplier will correlate multiple events in the Security platform.	24 x 7
Incident Cases	The supplier will manage each individual Incident Case in the Security platform.	24 x 7
Playbooks and Runbooks	The supplier will provide Customer specific response playbooks/runbooks that are developed and used within the Security platform.	24 x 7
Automated Processes	The supplier will use at its discretion, automated processes in the Security platform to speed up the threat analysis, response and containment to counter cyber threats in the Customers scope of service.	Normal Business Hours
Best Practice Collaboration	The supplier will use the Security platform to enable best practice collaboration with the Customer, including transparency over full case history, information shares, and documentation of response activities.	Normal Business Hours
Performance Measurement	The supplier will use the Security platform to track and measure performance, at the Suppliers discretion.	Normal Business Hours
Data Segregation	The supplier will provide Data segregation that is managed in the platform. A Customer specific environment will be created which will contain all Customer data. Only designated staff from the Supplier will have access and limited access will be provided to the Customer.	Normal Business Hours
Data Residency	The supplier will provide data residency in the United Kingdom. Data is held in Google Data Centres (europe-west2) based around London, UK.	24 x 7
Data Encryption	The supplier will enable Data hosted in the Security platform to be encrypted using AES-256 encryption. Data in transit is protected with TLS 1.2 or higher.	24 x 7
Data Security	The supplier will enable Data security supported by DDOS protection and WAF services, monitoring of the data centre is undertaken by Google 24/7 and the platform logs are additionally monitored separately under the Supplier service provision. All data in the service is backed up by Google	24 x 7

	Secure Operations. A daily full backup snapshot is taken. Any security incident involving Customer data in the Platform will be reported to the Customer.	
High Availability	The supplier will provide a security Platform that is configured to ensure high-availability.	24 x 7
Activity	**Threat Intelligence**	**Service Hours**
Native Threat Intelligence Support	The Supplier will support the Customer's Microsoft Security products that include a native threat intelligence feed. This feed can be enhanced through Microsoft, and the Supplier is not responsible for its provision.	24 x 7
Alert Data Enrichment	The Supplier will enrich alert data received from the security tooling using reputable threat intelligence provider feeds.	24 x 7
Multi-Source Threat Intelligence	The Supplier will source threat intelligence from multiple providers at the Supplier's discretion regarding selection.	24 x 7
Additional Feed Consideration	The Supplier will consider any additional feeds requested by the Customer, provided they are technically compatible with the Supplier's technology platform. The Supplier is under no obligation to accept additional threat feeds, and Customers may incur additional charges for integration and management.	Normal Business Hours
Critical National Infrastructure (CNI) Support	The Supplier will support Customers defined as part of Critical National Infrastructure (CNI), including any CNI-specific threat intelligence feeds, subject to additional onboarding and maintenance costs.	Normal Business Hours

5. Optional Bolt-On Services- Premier Tier

The Customer has the option to consume additional Services to the Security 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 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 additive to the Terms outlined in this document.

Bolt-On Services applicable at the Premier Tier are;

- Centre of Excellence

Service Definitions for all optional bolt-on services can be found here: [Service Definitions | ANS Service Definitions]

6. Incident Management

6.1. Incident Priority Table:

Affect	Business Impact		
	Minor	Moderate	Major
System/Service Down	P3	P2	P1
System/Service Affected	P4	P3	P2
User Down/Affected	P5	P4	P3

6.2. Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director/Vendor	Notification Frequency	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	6 Hours	GLASS Portal	1 Day
P3	4 Hours	1 Day	2 Days	None	GLASS Portal	10 Days
P4	1 Day	Never	Never	None	GLASS Portal	30 Days

For an Incident, "Response" is the time from when the ticket is first logged within ANS Glass to the time that the Supplier employee responds whether via an email, ANS Glass 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 updates at such frequencies as set out in the table above.

6.3. Cyber Security Incident Response and Escalation Table:

- Enterprise MDR Premier service only

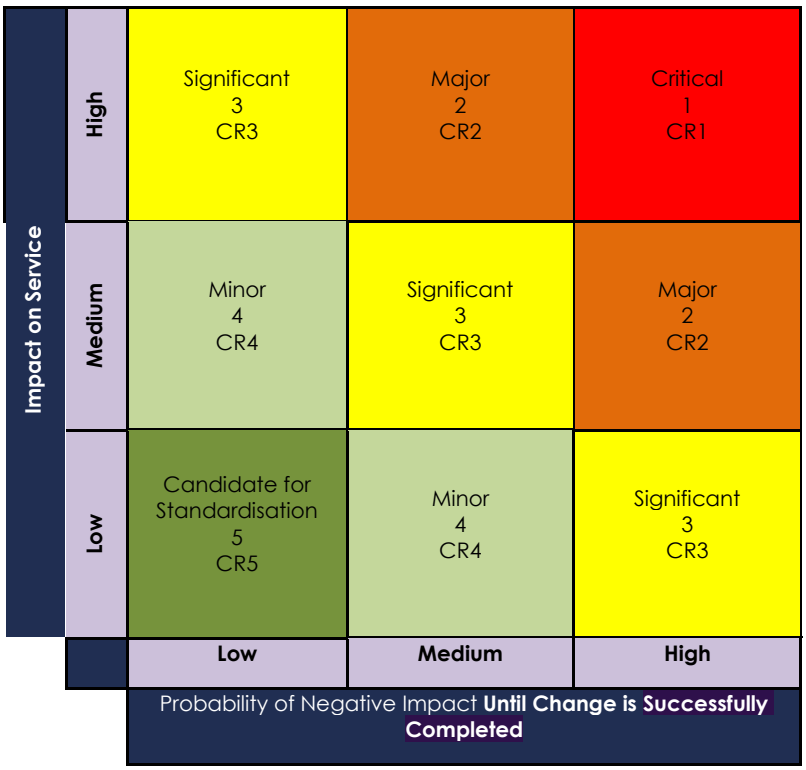
Security Incident Priority	Response	*Containment	Escalation
Priority 1: Confirmed malicious activity with active attacker presence or material impact.	15 mins (24/7)	24x7 containment response, subject to service scope and customer authority.	Service Desk SOC SOC Lead Service Lead Director of Security Operations
Priority 2: Medium: Confirmed malicious activity where impact is limited, contained, or time bound.	4 hours (24/7)		
Priority 3: Low - Suspicious or ambiguous activity that could represent early-stage attack behaviour.	1 Business Day (24/7)		

7. Change Management

All Changes require a Change Request Form to be completed on ANS Glass 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.

7.1. Change Risk Assessment Matrix



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

8. 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 2nd failure within a calendar month	1st Incident missed response time – 0% Service Credit 2nd Incident missed response time – 5% Service Credit 3rd 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.

9. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the applicable Terms should be consulted.

a. Issues resulting from misconfiguration by the Customer outside of the Demarcation Zone resulting in impact to the Customer's Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer of the scope of service resulting in impact to the Service.
c. Issues resulting from Unauthorised Access by the Customer of the scope of service.
d. End User or 1st line support.
e. Technical advice to any persons not listed as a named contact on the Customer's account.

f. Failure to meet the SLA due to outage(s) of the public cloud provider (Microsoft, AWS or Google).
g. Normal Changes requiring more than 2 hours of implementation time are excluded from the Service and will be subject to Additional Service Charges.
h. 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.
i. 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.
j. Applications without accurate services information for on-boarding the Service will be removed from scope and excluded from on-boarding.
k. 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.
l. 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.
m. The Supplier can only provide support for features that are in General Availability
n. Deployment and configuration of Log Analytics Workspace, Microsoft Sentinel, Data Connectors and Workbooks outside of the scope of service.
o. Provisioning and configuration of any Infrastructure or Operating Systems required to host Log Forwarders and Sentinel Platform components outside of the scope of service.
p. Security incident containment and/or remediation outside of the deployed Sentinel platform is dependent on additional service contract being in place for the specific technology.
q. Existing compromises prior to being live in service with the Supplier will be treated as a chargeable project to remediate in order to be accepted into service.
r. The Customers technology failing to respond to an execution command initiated by the Supplier to a Containment activity
s. Issues created by the Customer on systems that affect the scope of service that impact the ability for the Supplier to deliver the service.
t. The Supplier does not provide vendor integrated Digital Forensic Response retainer Services.
u. The Supplier will not include Digital Forensic Analysis where Incident Management is provided. Advice and guidance can be provided on selection of specialist 3rd party expertise.
v. Work done by the Supplier on the Customers environment remains the intellectual property of the Supplier.
w. The Supplier does not share any intellectual property created in support of the service with the Customer.
x. The service is not an IT Operational service monitoring or problem identification service and is not responsible for IT operational under performance issue identification.
y. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to additional Service Charges
z. The Supplier will not proceed without Customer authorisation where additional costs are to be raised. The Customer will hold all liabilities in this event.

In addition to the above exclusion, the following shall also apply in relation to the Premier Tier:

Exclusions In relation to MDR:

a. Any remediation resulting from any customer made changes not previously approved via ANS CAB unless agreed as part of Functional Engineer hours.
b. Rework to agreed changes will be outside of SLA, unless taken as part of functional engineers' hours.
c. Any 3rd party integrated applications not supported by Microsoft.
d. Customer ADO Management and underlying code.
e. Proactive monitoring of assets not supported by an additional ANS Managed Service.
f. The Supplier will be exempt from Service Level Failure in the event the Customer fails to support the Supplier in the development, approval and prioritisation of the backlog and its items.
g. The Supplier will be exempt from Service Level Failure in the event the Customer fails to remediate any issues that prevent The Supplier from being able to complete backlog items.

10. Customer Responsibilities

Including but 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 employees 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
    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 outlined in the Impact Assessment and any subsequently identified services 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 vendor support in place.
f. The Customer is responsible for all configuration backups outside of the 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 Assets and/or Supplier Assets from the address specified in the Contract. 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 Service Levels 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. In the case of testing any Enterprise MDR; The Customer may test the service once, post the full completion of onboarding. The Supplier requires 10 working days' notice for the test. The full results of the test must be shared with the Supplier for improvement and correction. Any subsequent testing is a chargeable event. All testing is subject to customer expense.
r. The Customer is wholly responsible for ensuring that the domain data, agent prompts, and any outputs generated by the agents meet the required standards. The Supplier's role is to facilitate the connection between technical configuration and domain expertise. However, the Customer retains full responsibility for domain knowledge and its application within the system. In instances where the agent does not produce responses that align with expectations, the Supplier will offer guidance to assist the Customer. Nevertheless, the ultimate responsibility for the quality of data and responses lies with the Customer.

Responsibilities In relation to MDR:

a. Provide the Supplier with technical access and relevant permissions to deliver the service under the scope of service, including providing the Supplier with authorisation and technical access to enable automated response for Containment and threat hunting. This includes the provision of Azure Lighthouse accounts in Microsoft tooling and access to other security tools in scope.
b. 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.
c. Assist the Supplier in the remediation of issues that may prevent operation of this Service.
d. Will 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.
e. Submit all service requests to the Supplier Service Desk, by means of the telephone or electronically by one of the designated named Customer's contacts.
f. Attend regular meetings scheduled at mutually convenient times.
g. Inform the Supplier, with a minimum of 5 working days, of any change that may impact the operation of the service.
h. 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.
i. Update the Supplier of changes to nominated individuals and associated contact details.
j. Support the Supplier with timely decision making in order to enable the appropriate countermeasures to a security incident to be deployed or enacted.
k. Will not hold the Supplier liable for any highly sophisticated or advanced threat actor attack that may occur that goes undetected by the tooling.
l. Will not hold the Supplier liable for any impacts of a malicious attack by any third party or malicious insider.
m. Apply all reasonable remediation recommendations to the in-scope 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. Standard Rate Card will apply.
n. Acknowledge and respond to incidents escalated by the Supplier with individuals nominated by the Customer to be included in the security event notification process.
o. Provide reasonable availability of Customer representative(s) when resolving a security related incident or request.
p. Ensure that all Customer Supported Assets are appropriately licensed and have Supplier recommended hardware/software and vendor support in place.
q. Ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
r. Report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels of Service Credits for Business-Critical Incidents raised via email.
s. Configure source technology to send logs into Microsoft Sentinel, unless the Supported Asset is under a managed contract with the Supplier.
t. Pre-authorise the Supplier to make changes to the Detection ruleset and policies without going through change control or Customer signoff. 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.
u. Acknowledge any changes by the Customer that disrupt the service will be subject to additional charges, at the standard rate card, to rectify and remediate.
v. Allow and enable the Supplier to electronically map any AWS or Azure environment for the purpose of incident response and assessment. Output can be shared with the Customer.

11. Assumptions

a. All Customer Supported Assets and production AWS and Azure 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 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 Enterprise Monitoring collector server.
e. The Customer will provide resource to work with the Supplier to on board 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. Work done by the Supplier on the Customers environment remains the intellectual property of the Supplier.
i. The Supplier does not share any intellectual property created in support of the service with the Customer.
j. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to additional Service Charges.

12. Pre-Requisites

a. On-Boarding Health check and documentation.
b. Platform and where applicable WMI access for all performance monitored services.
c. Registered Microsoft Partner of Record and/or AWS Associated Partner registration.
d. 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 Manager engagement.
f. Deployment of Supplier's accelerated Microsoft Sentinel deployment to agreed scope, defined in Statement of Work.

13. 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 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.

14. 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 agreement. Consequently, the Customer shall, prior to the 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.