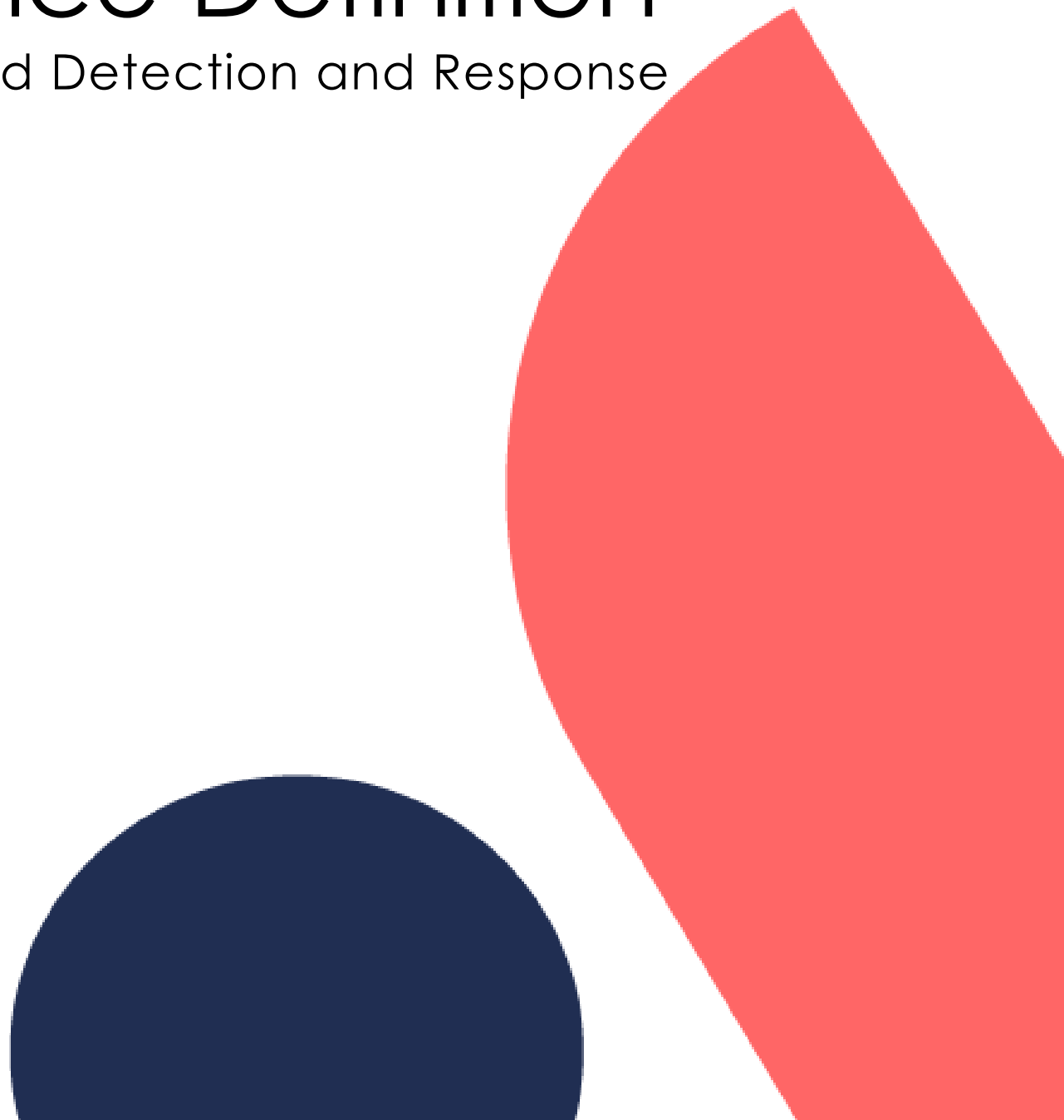
Service Definition

Extended Detection and Response



1. Operational Services

1.1. Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday (excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.2. Service Overview

Managed XDR (eXtended Detection & Response) is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response. The main benefit of Managed XDR is to identify threats and reduce the impact on organisations by isolating and remediating threats as soon as possible. The ANS Managed XDR Service is supported by our Security Operations Centre (SOC).

1.2.1. ANS Service

Service	Service Description	Service Hours
Incident Management		
Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P2, P3, P4 Security Incidents	Normal Business Hours
High Priority Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P1 Security Incidents	24 x 7
Security Incident Remediation and Advice	Provide advice, response, and containment of P2, P3 or P4 Security Incident	Normal Business Hours
High Priority Security Incident Remediation and Advice	Provide advice, response, and containment of P1 Security Incident	24 x 7
Service Desk - Non-Business Critical Faults	The Supplier provides access with relevant GLASS or phone contact details to the Supplier Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4) related to Microsoft Sentinel Platform, Microsoft Defender for Cloud and Microsoft 365 Defender issues.	Normal Business Hours
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Supplier Service Desk for critical system down scenarios (P1) only that are related to Microsoft Sentinel Platform, Microsoft Defender for Cloud and Microsoft 365 Defender issues.	24 x 7

Priority Escalation to Microsoft for faults	Priority escalation to Microsoft Premier Support for Microsoft Sentinel Platform, Microsoft Defender for Cloud and Microsoft 365 Defender issues.	Normal Business Hours
High Priority Escalation to Vendor	High Priority escalation to Microsoft Premier Support for Priority 1 business critical faults related to Microsoft Sentinel Platform, Microsoft Defender for Cloud and Microsoft 365 Defender issues.	24 x 7
Change Management & Advisory		
Data Connector Configuration	The Supplier will configure Microsoft Sentinel data connectors specified by the Customer.	Normal Business Hours
Log Forwarder Deployment and Configuration	The Customer will deploy and configure new Log Forwarder VMs as required with the Supplier providing support.	Normal Business Hours
Workbook Configuration	The Supplier will configure available workbooks to visualize and monitor insights from data connectors as specified by the Customer.	Normal Business Hours
Custom Workbook Configuration	The Supplier will create custom workbooks to visualize and monitor insights from data connectors.	Normal Business Hours
Notebook Configuration and Maintenance	The Supplier will create and maintain Notebooks used for Threat Hunting as specified by the Customer.	Normal Business Hours
Playbook Catalogue	The Supplier will provide the Customer access to a catalogue of all existing playbooks.	Normal Business Hours
Playbook Configuration and Maintenance	The Supplier will support the Customer to create and maintain Playbooks used for Security Orchestration, Automation, and Response (SOAR).	Normal Business Hours
Tuning of Sentinel Alerts	The Supplier will perform alert tuning over and above the Supplier's connector baseline on regular basis.	Normal Business Hours
Detection Rules	The Supplier will configure and customise Sentinel Detection rules as specified by the Customer.	Normal Business Hours
Microsoft Defender for Cloud (DfC) Capabilities (if applicable)		
Security Policy Enablement	The Supplier will enable Security Policy for available Industry & Regulatory standards.	Normal Business Hours
Security Policy Customisation	The Supplier will configure custom initiatives as specified by the customer.	Normal Business Hours
Vulnerability Management	The Supplier will help to prioritise and advise on vulnerability management findings within Defender for Cloud.	Normal Business Hours
Implementing Recommendations	The Supplier will document and then implement Defender for Cloud recommendations were agreed on with the customer.	Normal Business Hours
Implementing Regulatory Compliance	The Supplier will implement appropriate regulatory compliance in DfC.	Normal Business Hours

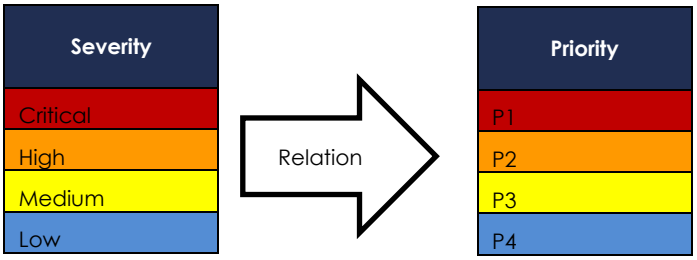
Regulatory Compliance Recommendations	The Supplier will document and then implement Defender for Cloud Regulatory Compliance recommendations were agreed on with the customer.	Normal Business Hours
Azure Firewall IDPS	The Supplier will configure and implement IDPS for the customer where plans are purchased.	Normal Business Hours
Azure Threat Intel	The Supplier will configure and implement Azure Threat Intelligence on the Azure Firewall for the customer where plans are purchased.	Normal Business Hours
Azure Arc	The Supplier will provide advice and guidance for the onboarding of up to 10 on-premises, or non-Azure cloud workloads. The customer will need to onboard any additional workloads.	Normal Business Hours
Environmental Settings	The Supplier will carry out or assist with Defender for Cloud Plan enablement with the agreement of the customer.	Normal Business Hours
Defender CSPM		
CSPM Queries	The Supplier will create CSPM queries and run them on customer request.	Normal Business Hours
Monitoring & Event Management		
Platform Monitoring	The Supplier will monitor the platform providing bespoke workflows, thresholds, availability, and performance.	24 x 7
Service Management & Security Operations		
Microsoft Sentinel Platform Access	Customer access to Microsoft Sentinel Platform deployment including configured connectors, workbooks, and notebooks.	24 x 7
Microsoft Defender for Cloud Access	Customer access to Microsoft Defender for Cloud deployment.	24 x 7
GLASS Portal Access	Customer access to ANS GLASS portal providing visibility of all Service-related tickets, performance dashboards and Cloud Score.	24 x 7
Problem Management	ANS Problem Management processes are adhered to for incident, change and event reduction. Problems are reviewed during the Service Management Review.	24 x 7
Customer Success	The Supplier will provide a Customer Success Manager	Normal Business Hours
Customer Success Architect	The Supplier will provide a Customer Success Architect responsible architectural validation and platform efficiency focused on continuous improvement of the Customer's DX Score	Normal Business Hours
Service Reviews	Service Management Review (SMR) Reports will be distributed at regular intervals and discussed via a meeting between the Supplier and the Customer. The SMR Report will cover the previous period. Please refer to your Service Statement for SMR frequency and meeting type.	Normal Business Hours
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents	

	(regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	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.	Normal Business Hours
Change Management Process	The Supplier will take full ownership of the Change Management Process for the Microsoft Sentinel Platform	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes for the Microsoft Sentinel Platform	24 x 7

1.3. Security Incident Management

A Security Incident is a pattern of potentially malicious activity that implies an identified threat to an information system, violates acceptable use policies, or circumvents standard security practices. The Supplier classifies incidents into four threat severity ratings: Critical, High, Medium, and Low.

1.3.1. Threat Severity Ratings:



1.3.2. Incident Response and Escalation Table:

Incident Priority	Threat Severity Rating	Response SLA	Escalation Notification	Notification Type
P1	Critical	15 Minutes	Immediate	Telephone Call
P2	High	1 Hour	None	Email/GLASS
P3	Medium	4 Hours	None	Email/GLASS
P4	Low	1 Day	None	N/A
P5	Question Query	2 Days	None	N/A

For an Incident, "Response" is the time from when the ticket is first logged within the Supplier ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call (dependant on Priority).

For 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 by email or GLASS Portal updates at such frequencies as set out in section 1.4.2 below.

Incident Resolution is handled by the Change Authority of the Supported Asset under investigation.

1.4. Security Incident Remediation

Remediation steps for Security Incidents are shared with the Customer by the Supplier. Resolution of and carrying out remedial steps is the responsibility of the Change Authority of the Supported Asset under investigation.

If the Supported Asset is under a Managed contract with the Supplier, then the Service Levels of that contract will comply and the Supplier will remediate via the Suppliers Change Management Process.

Where the Customer is the Change Authority then the Incident will be functionally escalated (assigned) to the Customer to deliver any required remedial actions via Change Management.

1.5. Platform Incident Management

1.5.1. Platform 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

1.5.2. Platform Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	15 Minutes	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	None	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
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident related to the Microsoft Sentinel Platform, "Response" is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call (dependant on Priority).

For 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 by email or GLASS Portal updates at such frequencies as set out in the table above.

1.6. Change Management

All Changes require a Request for Change (RFC) form to be completed on the Suppliers GLASS Portal and submitted detailing the required Change. The Supplier will reject unapproved or incomplete RFC forms. Changes will follow the Change Management Process as defined in the ANS 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) and/or a major Security Incident where the Supplier deems appropriate.

1.6.1. Change Risk Assessment Matrix

Impact on Service	Probability of Negative Impact **Until Change is Successfully Completed**		
	Low	**Medium**	**High**
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

1.6.2. 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 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 this Contract will be completed by the Supplier at no additional cost.

2. 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 15 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.

3. Exclusions

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

a. Issues resulting from misconfiguration by the Customer outside of the Supported Assets resulting in impact to the Service.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Supported Assets resulting in impact to the Service.
c. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets.
d. End User or 1st Line support.
e. Technical Advice to any persons not listed as a Named Contact.
f. Failure to meet SLA due to Public Cloud provider outages.
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 the Supplier ITSM Tool 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. Deployment and configuration of Log Analytics Workspace, Microsoft Sentinel, Data Connectors and Workbooks outside of the Supported Assets.
k. Provisioning and Configuration of any Infrastructure or Operating Systems required to host Log Forwarders and Sentinel Platform components.
l. 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 e.g., ANS CoManaged Cloud.

4. 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 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 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 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 Request for Change (RFC) 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 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 or region 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. Customers are responsible for racking and installing any physical on-premises Log Forwarder infrastructure (if applicable), and any subsequent configuration of on-premise Log Forwarder VMs.
q. Configuration of source technology sending logs into Microsoft Sentinel, unless the Supported Asset is under a Managed contract with the Supplier.
r. The Customer shall be responsible for any Licensing requirements.

5. Assumptions

a. All Customer Supported Assets and Azure Accounts within the Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
c. All Customer specific pre-requisites have been completed before contract commencement.
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. Some services and configurations incur additional costs at the customers expense e.g., Defender Cloud Security Posture Management (CSPM).

6. Pre-Requisites

a. On-Boarding Health Check and Documentation
b. Deployment of Supplier's Microsoft XDR Accelerator to agreed scope defined in Statement of Work
c. Platform and where applicable WMI access for all monitored services
d. Registered Partner of Record
e. Administrative Access Permissions for ANS Engineers on supported Subscriptions

7. Partner Admin Link

ANS' Managed Cloud for Azure incorporates Microsoft Signature Cloud Support for any issues that require escalation to Microsoft. In order for this to be able to be fulfilled, Microsoft leverage information collected from the Partner Admin Link (PAL) system to assign back-end support rights. As such ANS must be registered as the digital PAL on any Subscriptions 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 ANS to be registered as the PAL and must have either Owner or Contributor rights to all subscriptions and resources that contain or contribute to assets under support or management for the entire duration of this agreement.