



# Service Definition

Business Applications | Standard

# 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

### 1.1.1. ANS Service

Service	Service Description	Service 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.	24 x 7
Change Management & Advisory		
Change Guidance & Configuration Validation	The Supplier provides access to Change Advisory for: <ul style="list-style-type: none"> <li>• Configuration</li> <li>• Change Validation</li> <li>• Design</li> </ul>	Normal Business Hours
Expert Access	The Supplier provides access to Business Application Experts for question/query Service Requests	Normal Business Hours
Service Operations		
GLASS Portal Access	Customer access to ANS GLASS portal providing visibility of all Service related tickets and performance dashboards.	24 x 7
Change Management Process	On request, the Supplier will take full ownership of the Change Management Process for the Customer Supported Assets. Changes are charged per hour and will be deducted from pre-paid hours or invoiced ad-hoc.	Normal Business Hours

## 1.2. Incident & Service Request Management

### 1.2.1. 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

### 1.2.2. 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
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident, "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 or in person. 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.

The first 30 minutes of all incidents and service requests are included within this service at no extra charge. With the exception of infrastructure related incidents for CSP customers, subsequent support may be subject to additional charges or use of the customers pre-paid hours. Any such charges will be pre-agreed with the Customer prior to the commencement of work.

## 1.3. 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.

### 1.3.1. 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		

### 1.3.2. 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
P1 Incidents	100% of incidents responded to within 30 minutes – Normal Business Hours (24x7 CSP infrastructure only)
P2 Incidents	100% of incidents responded to within 1 Normal Business Hour.
P3 Incidents	100% of incidents responded to within 4 Normal Business Hours.
P4 Incidents	100% of incidents responded to within 1 Working Day.
P5 Incidents	100% of incidents responded to within 2 Working Days.
Root Cause Analysis	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days.

### 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 Customer Supported Assets resulting in impact to the Customer Supported Assets.
- b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
- c. Issues resulting from misconfiguration or development by the Customer and/or the Customers chosen 3<sup>rd</sup> Party Application provider.
- d. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets.
- e. End User or 1<sup>st</sup> Line support.
- f. Technical Advice to any persons not listed as a Named Contact.
- g. Failure to meet SLA due to Public Cloud provider outages.
- h. All Changes will be subject to Additional Service Charges.
- i. 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.
- j. 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 charges.

### 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 (where required)
  - f. The Customer shall check LED status of equipment onsite (where required)
- 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 (where required) 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 overall responsible for Data Backups and the Health of Data Backups for Recovery unless this Service is purchased with the Suppliers Managed Backup service.
- 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. 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.

## 5. Assumptions

- a. All Customer specific pre-requisites have been completed before contract commencement.

## 6. Pre-Requisites

- a. On-Boarding Health Check and Documentation.
- b. Registered Partner of Record (where required).
- c. Administrative Access Permissions for ANS Engineers on supported Subscriptions/Accounts and Customer Supported Assets.

## 7. Partner of Record

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 of Record (PoR) system to assign back end support rights. As such ANS must be registered as the digital PoR 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 PoR on all Subscriptions that contain or contribute to assets under support or management for the entire duration of this agreement.