Service Definition

Edge Compute Infrastructure

1. Operational Services

1.1. Operational Services

1.1.1. 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	09:00 -17:30, Monday to Friday (excluding bank holidays in England and Wales)
Emergency hours	17:31 to 08:59 Monday to Friday including bank holidays in England and 17:31 Friday to 08:59 Monday including bank holidays in England and all of Saturday and Sunday in England.
Working Day	8.5 Normal Business Hours
24 x 7	24 hours a day, 7 days a week
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	Supplier's change advisory board
CAB Approval	change approval of the CAB required as part of the Change Management Process for Normal Changes.
Change	any addition, modification, or removal of any component or configuration that has the potential to affect any part of the System directly or indirectly.
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	the party receiving the support & maintenance services from the Supplier.
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 Supported Assets	Any resource that is provisioned by the Supplier to provide the Customer with Edge Compute Infrastructure

Demarcation Zone	Infrastructure or solutions being provided as Customer Supported Assets by the Supplier. Anything outside of this is considered out of scope of the Service.
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.
Escalation Manager	Supplier's technical escalation point, typically a Supplier Apex Squad Leader.
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	any failure of any part of the solution to perform in accordance with its intended functionality; or any event or threat of an event that is not part of the standard operation of any part of the system and that causes, or may cause, an interruption to, or a reduction or adverse change in, the quality or functionality of any part of the System.
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.
Normal Changes	Change that is not a Standard Change or Emergency Change. Normal Change goes through the Change Management Process, including assessment, authorisation and scheduling.
Project Change	Change delivered by way of the Supplier's Professional Services.
Resolution	the criteria for resolution are agreed as part of the impact assessment. When the criteria are met, the incident will be marked as resolved and we will contact you to confirm the authority to close the incident.
Root Cause Analysis	a process used to identify the underlying cause(s) of Incidents or problems.
Security Incident	an Incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, or security.
Service Desk	the facility to be provided by the Supplier in accordance with this Service Level Agreement (SLA) to receive and respond to support requirements from the Customer.
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.
Service Management Review	regular meeting delivered by the Supplier focused on performance and value of the Managed Services contracted.
Standard Change	a pre-authorised Change that is low risk and follows a documented process for implementation.
SOW	Statement of Work outlining intended professional services engagement and outcomes,
Supplier	ANS Group Limited.
Support Requirement	a formally logged request or Incident initiated by the Customer, that requires technical investigation, remediation, or advisory action by the Supplier.
System	the functionally related group of elements including hardware and software provided by the Supplier.
Valid Supported Configuration	a configuration of an IT service or component that is formally approved, tested, and supported by the Supplier and vendor
WMI	Windows Management Instrumentation.
3rd Party Data Centre Providers	any data centre provider that is not managed and maintained by the Supplier. Responsibility sits with the Customer for any 3rd Party Data Centre Provider where the Supplier's Edge Compute resides.

1.2. Service Description

The Edge Compute Service provides hardware infrastructure on Customer premises with remote support providing essential services. It is designed to deliver robust, low-latency computing capabilities at, or near the data source, enabling real-time processing and improved operational efficiency.

1.2.1. ANS Service

Service	Service Description	Service Hours
Incident Management		
Telephone and Remote diagnostics for faults	The Supplier is responsible for conducting incident management via ANS Glass, telephone, Microsoft Teams, mail, and remote connection for Priority 2-5 support in Normal Business Hours.	Normal Business Hours
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4).	Normal Business Hours
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Service Desk for critical system down scenarios (P1) only.	24 x 7

Change Management & Advisory		
Ops Advisory & Architecture Validation	Engineers provide hands on validation and design guidance for new projects and applications.	Normal Business Hours
OS Patch Management	Where purchased, the Supplier shall patch Customer Supported Assets in line with the agreed schedule. Assets are grouped in weekly cycles, and the process is repeated monthly. Monthly patch status report of all assets within the patching cycle under the Supplier service. Critical patch release service in the event of the Supplier identifying a Supplier urgent critical patch being released, the Supplier reserves the right to push out the patch via an Emergency Change process.	24 x 7
Workload Configuration	The Supplier will provide access to ANS Glass for configuration changes on the operating system for Disk, CPU & RAM.	24 x 7
Backup Setup & Configuration	Where backups are purchased as part of the solution, the Supplier will setup and configure the initial requirements via a professional service or setup engagement, any new backup requirements to be configured during the term of the Services can be actioned by the Customer using ANS Glass or via a Change. The Supplier will provide access to self-service portal for the self-service management of backups, offering the ability to create new backups and restore backups. The Supplier provides 24/7 access with relevant phone contact details to the Service Desk for critical system down scenarios (P1) only.	Normal Business Hours
Access Control List Configuration & Management	The Supplier will provide access to ANS Glass to configure and manage access control lists to suit the Customer's requirements.	24 x 7
VPN Configuration & Management	The Supplier will provide the Customer access to ANS Glass to configure and manage standard VPNs.	Normal Business Hours
High Availability & Recovery		
HA Configuration	Where a high-availability solution has been deployed and purchased, the Supplier will configure and manage the availability of the solution at the infrastructure level.	Normal Business Hours
HA Management	Where a high-availability solution has been deployed, and purchased, the Supplier will help manage failover of resources during P1 Incidents & Supplier managed patching.	24 x 7
Monitoring & Event Management		
Platform Monitoring	The Supplier will monitor the platform providing bespoke workflows, thresholds, availability and performance.	24 x 7
Performance Tuning and Diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customer solution achieve better and more consistent performance.	Normal Business Hours

Backup Tooling & Monitoring	The Supplier will monitor overrunning backup jobs and failures including remediation via rescheduled backups.	Normal Business Hours
Customer Monitoring & Event Management		
Infrastructure Monitoring	The Supplier will monitor the Edge Compute infrastructures health and will provide alerting for availability and capacity using pre-defined and appropriate thresholds to alert both support teams and the customer of developing issues. Changes can be made to alert configurations and thresholds on request.	24 x 7
Performance Tuning and Diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes within the virtual machine level that can help the Customer's solution and backups to achieve better and more consistent performance.	Normal Business Hours
Protect & Recover		
Backup & Recovery	Where backups are purchased as part of the Service, the Supplier will setup backups where requested by the Customer and help recover from backup where requested. A self-service portal will also be provided.	Normal Business Hours
High Priority Backup Restores	Where backups are purchased as part of the Services, the Supplier will commit to backup restores of customer supported assets upon a Priority 1 (P1) Incident being raised with the Supplier.	24 x 7
Test Backup Restores	The Supplier will commit to testing backup restores of Customer Supported Assets upon an Incident being submitted by the Customer to the Supplier. This Service is subject to fair use, with a maximum of one test per quarter.	Normal Business Hours
Service Operations		
Customer Portal	Customer access to ANS Glass providing visibility of all Service-related tickets, alerts and performance dashboards. ANS Glass also facilitates automations of platform provisioning and management of resources	24 x 7
Named Account Contacts	The Supplier will provide a named account manager and/or a Customer Success Manager. Confirmation on named account contacts will be provided during contract agreement/service onboarding.	Normal Business Hours
Service Reviews	Service Management Review (SMR) reports will be distributed at regular Intervals, as agreed by the Customer and the Supplier and discussed via a meeting between the Supplier and the Customer. The SMR report will cover the previous period.	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	Normal Business Hours

	Supported Assets. Where appropriate, the Supplier will participate in a customer led Change process where needed.	
Change Management Process	The Supplier will integrate the release pipeline into the Supplier's Normal Change process giving the Customer access to Change Approval for production release management.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 x 7
Physical Asset Protection		
Hardware – Non Business Critical Faults	Where physical hardware is running in N+1 or highly aailable configuration the Supplier will replace hardware non disruptively.	Normal Business Hours
Hardware - 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).	24 x 7
Infrastructure Services	The Supplier will manage the platform infrastructure, including software and firmware versions as per vendor requirements. Vendor escalation will be provided where required at the Supplier's discretion.	Normal Business Hours
Network Management	The Supplier will upgrade firmware upon vendor requirements. Vendor escalation will be provided where required.	Normal Business Hours
Customer Success		
Customer Success	The Supplier will provide a Customer Success Manager.	Normal Business Hours
Customer Success Plans	The Supplier will provide a success plan to align service delivery to Customer goals, providing a clear roadmap for action with regular progress updates via the Service Management Review (SMR).	Normal Business Hours

1.3. Incident Management

An Incident is "an unplanned interruption to the Customer hosted Solution or a reduction of the performance in the solution." Incidents have a wide scope and can fall into different classification and prioritisation levels. In contrast, a Request is a "pre-defined, pre-authorised request from a user for something to be provided."

In the event an Incident or Request is raised, the Service Desk will ensure it is logged and categorised before triaging using the Incident and Request Classification process. Incidents can be classified into categories; Major, Moderate and Minor and prioritised P1 to P5. Each category of classification has an SLA for Response time and Resolution target.

1.3.1. 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

1.3.2. Incident Response and Escalation:

For an Incident, "Response" is the time from when the ticket is first logged within ANS Glass to the time that the Supplier responds whether via an email, ANS Glass update, telephone call or in person. P1 incidents must be telephoned in, for a detailed process flow, please refer to the 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.

Target Resolution KPI applies to Support Requirements where the root cause falls within the Supplier's responsibility. The Target Resolution KPI is satisfied when the Support Requirement is either resolved or a time frame and plan for full resolution has been communicated to the Customer. From the time of Response until resolution, updates shall be provided to the named contacts and/or escalation contacts on the Customer's account by email or by ANS Glass updates at such frequencies as set out in the table above. Measurement of SLA response and other timescales will not commence until the appropriate information to allow investigation has been received. Measurement of the SLA response and other timescales will be stopped during periods where the incident is back with the Customer or where an action is required outside of the Supplier team.

Priority	Response SLA	Specialist Review	Escalation Manager	Notification Frequency	Target Resolution KPI
P1	30 Minutes	2 Hour	Immediate	Hourly Email	4 hours
P2	1 Hour	4 Hours	1 Day	GLASS Portal	1 Day
P3	4 Hours	2 Days	4 Days	GLASS Portal	10 Days
P4	1 Day	Never	Never	GLASS Portal	30 Days
P5	2 Days	Never	Never	GLASS Portal	None

1.4. 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.

1.4.1. 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**		

1.4.2. 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.

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 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 Charge (excluding licences) and in any event, shall not exceed 10% of the monthly Charge (excluding licences) 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. Responsibility Matrix

Responsibilities	ANS	Customer
Purchase of Hardware Infrastructure	✓	
Architecture and build	✓	
Remote Installation of Hardware Infrastructure	✓	
Base OS installation	✓	
IP configuration	✓	✓
Network Infrastructure		✓
3rd Party Data Centre partnership		✓
Management above VM level (including OS)	✓	✓

Availability and health monitoring	✓	
Line of business and third-party applications		✓
Onsite support	✓	✓
Replacement of failed Hardware	✓	✓

4. 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 supported elements of their solution (which are not agreed in writing with ANS and tested for compatibility prior to making such changes) resulting in impact to the solution.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the solution resulting in impact to the Service.
c. Issues within, or which are caused by the Customer's code.
d. Issues created by the Customer's applications not being configured in a high availability configuration e.g. single SQL servers.
e. Issues resulting from unauthorised access as a result of the Customer's actions
f. Issues created by the Customer making changes to the solution that impacts the ability of the Supplier to deliver the service.
g. Any issues caused where the software/hardware and/or equipment provided by the Customer does not conform to the design and/or specification requirements agreed in writing with the Supplier.
h. Any issues caused by negligence on the part of the Customer, its employees, servants or agents and third-party vendors.
i. For Supplier-provided dual site solutions, the Supplier is not permitted by the Customer to carry out annual disaster recovery failover testing.
j. The availability of any Application Programming Interface (API) written and provided by the Supplier as part of the Services.
k. End User or 1st line support.
l. Technical advice to discuss account specific details including technical advice to any persons not listed as a named contact on the Customer's account.
m. Project Changes are excluded from the Service and will be subject to additional charges. Project charges are recorded within ANS Glass for information and approval purposes only.
n. Emergency Changes that are not a direct output of a priority 1 incident may be subject to additional charges.
o. Existing compromises of the Customer infrastructure prior to being migrated and live in service with the Supplier will be treated as a chargeable project to remediate in order to be accepted into service.
p. Where Service Credits are directly associated to or linked to a minimum service level percentage, there must be a minimum of 4 tickets, or the Service Credit is excluded.
q. Terms for any additional support services provided by the Supplier to the Customer are not included in this service
r. Normal Changes requiring more than 2 hours of implementation time are excluded from the Service and will be subject to additional charges.
s. Issues resulting from 3rd Party Data Centre Providers.

5. 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 is responsible for all backups outside of those supported by the Supplier without exception.
e. The Customer is responsible for any issues caused by third-party software installed by the Customer and/or the support of applications that do not feature on the Suppliers supported applications list, or as part of the agreed intended functionality of the solution which is then compromised
f. The Customer is responsible for completing a Change Request Form in accordance with the Change Management Process.
g. The Customer shall ensure an on-going availability of a suitable internet connection on the customer side
h. 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.
i. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the System, including environmental changes. Failure to do so may result in additional charges to the Customer.
j. 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 P1 Business-Critical Incidents raised via email.
k. 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.
l. The Customer is responsible for applications not installed by the Supplier.
m. Unless purchased, the Customer is responsible for the security and integrity of the operating system and application stack.
n. The Customer takes responsibility for the management of any network infrastructure from the point of the external connection terminating with the external interface of a supplier-operated Layer 3 device (Edge Router, Firewall, VPN Terminator) within the data centre.
o. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support in place.
p. The Customer shall ensure that all relevant Customer employees have access to and have read the Managed Services Handbook.
q. 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 from the address specified in the Contract. Any asset that has been moved without notification to the Supplier will be subject to additional charges (for any hardware and/or engineering time) which will be notified to the Customer.
r. Customer will be responsible for arrangement for providing onsite hands and eyes support. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to additional charges (for any hardware and/or engineering time) which will be notified to the Customer.
s. 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.
t. The Customer has the responsibility to own the relationship with the 3rd Party Data Centre and control any associated management of hardware services or products that are not covered by the Supplier support agreement.

6. Assumptions

a. The relevant System is covered by a valid software maintenance and support agreement in line with applicable Service Levels.
b. The relevant System is in a Valid Supported Configuration at contract commencement.
c. All Customer specific pre-requisites have been completed before contract commencement
d. The Customer will provide resource to work with the Supplier to on-board the Service, and assist with on hands maintenance tasks as required
e. Management of service connectivity is the responsibility of the individual connectivity provider (PSN, MPLS, network provider etc)
f. Work done by the Supplier on the Customer environment remains the intellectual property of the Supplier
g. The Supplier does not share any intellectual property created in support of the Service with the Customer
h. Installation of the base OS and initial IP configuration will be performed by the Supplier. Operating system support will not be offered post initial deployment of the System.
i. Support of applications is only up to the operating system layer that is part of the System.
j. The Customer will provide a suitable specification platform, operating system for the enterprise monitoring collector server.

7. Pre-Requisites

a. Completion of the Supplier's Enterprise Pre-Launch Questionnaire (ELQ).
b. Administrative relevant access permissions for all patching and monitored services.
c. Administrative relevant access permissions for Supplier engineers on supported devices where required.
d. Supplier will grant access to the Customer to ANS Glass.
e. All Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with the applicable Service Levels.
f. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract commencement.
g. Platform and where applicable WMI access for all monitored services
h. Administrative access permissions for Supplier's engineers on supported subscriptions / accounts