Service Definition

eCloud Private (Enhanced)

1. Operational Services

1.1. Terms and definitions

Term	Definition
Normal Business Hours	09:00 - 17:30, Monday to Friday (excluding bank holidays).
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.
Customer	The party receiving the support & maintenance services from ANS.
Supplier	ANS Group Limited.
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 which is provided by the Supplier.
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.
Service Desk	The facility to be provided by ANS in accordance with this Service Level Agreement (SLA) to receive and respond to support requirements from the Customer.
Supplier ITSM Tool	An IT Service Management platform provided by the Supplier for use by the Customer to raise incident and change requests via the ITSM tool.
System	The functionally related group of elements including hardware and software provided by ANS.
Resolution	The criteria for resolution are agreed as part of the impact assessment. When the criteria is met, the incident will be marked as resolved and we will contact you to confirm the authority to close the incident.

1.2. Operations Baseline

Service	Service Description	Service Hours
Incident Management		
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Supplier's 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 Supplier's 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	The Supplier shall patch supported assets in line with the agreed schedule. The agreed schedule is set in the Enterprise Pre-Launch Questionnaire (ELQ) or Low-Level Design (LLD). For Microsoft Servers, if no schedule is agreed in the ELQ or Low-Level Design the Supplier's default schedule will be applied. The Supplier will update Linux server installations upon the customer's request working to an agreed process with the Customer.	24 x 7
OS Configuration	The Supplier will provide a Web Portal for configuration changes on the Operating System for Disk, CPU & RAM.	24 x 7
Software Configuration	The Supplier will update supported applications within the Operating System upon the Customer's request working to an agreed process with the Customer. This is limited to software installed by the Supplier only.	Normal Business Hours
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 the self-service portal 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 Supplier's Service Desk for critical system down scenarios (P1) only.	Normal Business Hours

Access Control List Configuration & Management	The Supplier will provide access to a Web Portal 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 a Web Portal to configure and manage standard VPNs.	Normal Business Hours
High Availability & Recovery		
HA Configuration	Where a high-availability solution has been deployed the Supplier will configure and manage the availability of the solution at the infrastructure level.	Normal Business Hours
Failover Management	Where a high-availability solution has been deployed, 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 platform 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 thresholds on request.	24 x 7
Performance Tuning and Diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes at the infrastructure level that can help the Customer's solution and backups to 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
Protect & Recover		
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
Backup & Recovery	Where backups are purchased as part of the Services, 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
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. Subject to fair use (Max Quarterly).	Normal Business Hours
Antivirus	Where Antivirus is licensed and purchased through the Supplier, the Supplier will deploy and manage required policies.	Normal Business Hours
Service Operations		

Web Portal	Customer access to a web portal providing visibility of all Service-related tickets, alerts and performance dashboards.	24 x 7
Named Account Contacts	The Supplier will provide a named Account Manager and a Customer Success Manager. Confirmation on named account contacts will be provided during contract agreement/service onboarding.	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. Feature Requests are delivered as Project Changes.	Normal Business Hours
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 (see 3.2).	24 x 7
Physical Asset Protection		
Hardware – Non Business Critical Faults	Where physical hardware is running in N+1 or Highly Available 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 infrastructure as a service, including software and firmware versions as per Vendor requirements. Vendor escalation will be provided where required.	Normal Business Hours
Network Management	The Supplier will upgrade firmware upon Vendor requirements. Vendor escalation will be provided where required.	Normal Business Hours

2. Incident Management

An Incident is "An unplanned interruption to the IT service or a reduction in the quality of the IT service." 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." While incidents deal with needs, requests deal with wants.

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 P4. Each category of classification has an SLA for Response time and Resolution target.

2.1. Incident Priority

The information above is simplified and displayed visually in the table below:

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

2.2. Incident Response and Escalation

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, Portal update, telephone call or in person. P1 incidents must be phoned 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 ANS'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 by email or Web Portal 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 an ANS team.

Priority	Response SLA	Specialist Review	Customer Success Manager	Notification Type	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	1 day	Web Portal	1 Day
P3	4 Hours	1 Day	2 Days	Web Portal	Not applicable
P4	1 Day	Never	Never	Web Portal	30 Days

3. Availability

The Supplier shall ensure that Availability of the system in any month is not less than 99.75%.

Availability Service Credits are calculated as a percentage of the monthly Base Charge for non-availability of the System and in any event shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose.

*Availability is calculated utilising the following formulas:

Agreed Service Time: AST = 24*7-(SW+M)

Availability: $A = \frac{AST- Downtime}{AST} * 100$

“Downtime” means non-availability of one or more of the primary functions of the System but excludes:

- Any agreed downtime, Scheduled Work (SW) or Planned Maintenance (M).
- Any downtime due to Emergency Changes.
- Any agreed downtime due to failover in a disaster recovery scenario.
- Any downtime attributable to the Customer or its customers’ actions or omissions.
- Any downtime is due to issues in Customer’s data integrity, system software, the operating system, vendor supplied patches and/or application code.
- Any downtime is due to application load and/or traffic spikes.
- Any downtime caused by an application operated by the Customer on its system (in circumstances where there has been failover and the System performed as anticipated).
- Capacity management for which the Customer is responsible.
- Where the Customer’s applications are not configured in a high availability configuration e.g. single SQL servers.
- Where the Customer’s System fails to respond to the Supplier’s monitoring tool.

This only includes downtime of the network, hardware, virtualisation and base operating system components.

Key:
Agreed Service Time (AST)
Scheduled Work (SW)
Planned Maintenance (M)

4. 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.	None	No 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
Availability of System	100%	99.75%	Availability 99.75% to 99.51% - 2% Service Credit per month 99.50% to 99.26% - 5% Service Credit per month 99.25% or less – 10% Service Credit per month

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.

5. Exclusions

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

a. Issues resulting from misconfiguration by the Customer outside of the System (which are not agreed in writing with ANS and tested for compatibility prior to making such changes) resulting in impact to the System.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the System resulting in impact to the System.
c. Any issues caused by the Customer's applications not being configured in a high availability configuration e.g. single SQL servers.
d. Any issues caused by the Customer making changes to the System.
e. 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 ANS; this shall include the requirement for the Customer to have an ANS-provided firewall device as part of the solution design.
f. Where the Services are for an ANS provided dual site solutions, the Supplier has not been permitted by the Customer to carry out annual DR Failover Testing; and
g. The availability of any Application Programming Interface (API) written and provided by the Supplier as part of the Services.
h. End User or 1st Line support.
i. Technical advice to discuss account specific details including technical advice to any persons not listed as a Named Contact.
j. 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.

6. Customer Responsibilities

Including but not limited to:

a. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed.
b. 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 is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support is in place
c. The Customer is responsible for all configuration backups outside of those supported by ANS without exception.
d. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
e. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier).
f. 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.
g. 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 Service Charges (as referred to in the Contract).
h. 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.

i. 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.
j. The Customer is responsible for applications not installed by the Supplier.
k. The Customer is responsible for the security and integrity of the operating system and application stack unless purchased as an additional service.

7. Assumptions

a. The relevant System provided under the Contract is covered by a valid software maintenance and support agreement in line with the Contract Service Levels.
b. The relevant System provided under the Contract is in a Valid Supported Configuration at the point of contract start date.

8. Pre-requisites

a. Completion of the Enterprise Pre-Launch Questionnaire (ELQ).
b. Management access for all patching and monitored services.
c. Administrative Relevant Access Permissions for ANS Engineers on supported devices where required.
d. Supplier will grant access to relevant ITSM tool.
e. All Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
f. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.