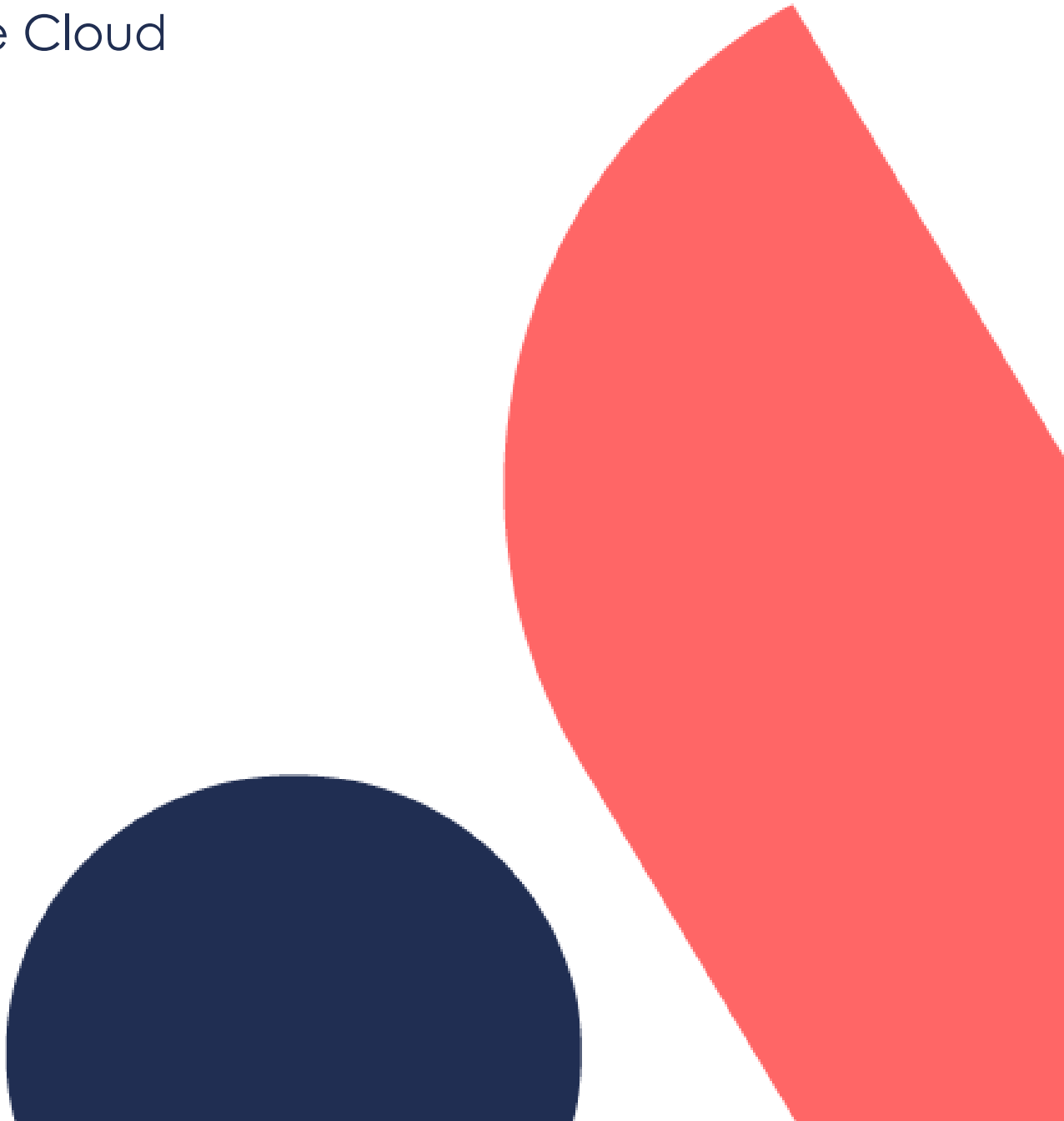
Service Definition

Private Cloud



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
24x7	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 is 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 Suppliers 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 Sevices 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	Normal Business Hours

	contact details to the Supplier's Service Desk for critical system down scenarios (P1) only.	
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 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 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.	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/or 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.	Normal Business Hours
Network Management	The Supplier will upgrade firmware upon Vendor requirements.	Normal Business Hours

2. Incident Management

2.1. Incident Priority

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

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

For an Incident, "Response" is the time from when the ticket is first logged (within the Customer Portal or by phone call) to the time that the Supplier responds with a suitably qualified person whether via an email, Customer Portal update, telephone call or in person. 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.

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.

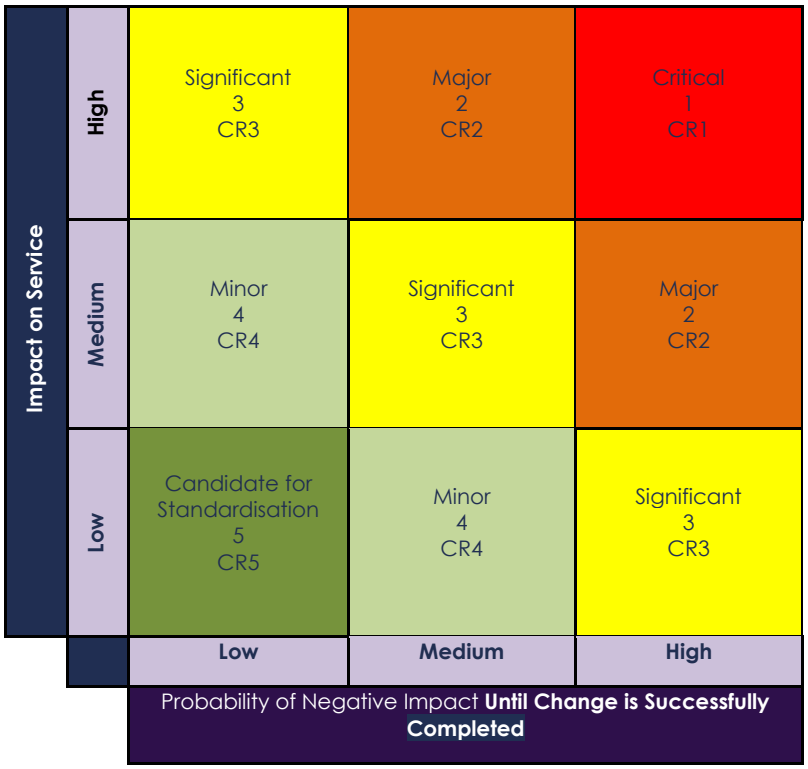
From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or Web Portal updates at such frequencies as set out in the table above. Measurement of SLA response and other timescales will not commence until the appropriate information 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.

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.

3.1. Change Risk Assessment Matrix



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 Services within the scope of this document will be completed by the Supplier at no additional cost.

4. 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, virtualization and base operating system components.

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

5. 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
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% or 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.

6. 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 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 eg 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. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges (as referred to in the Contract)
k. Project Changes (Normal CR6) are excluded from the service and will be subject to Additional Service Charges(as referred to in the Contract). Project Changes are recorded within the Supplier ITSM Tool for Informational and approval purposes only.
l. Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges (as referred to in the Contract)e.g. Poor planning from a Customer Managed Project.
m. 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.
n. Where OS patching has failed to install patches on Windows Servers, the patch will retry for install in the next scheduled maintenance window until the patch is successful or removed from availability on the WSUS catalogue of updates.

7. 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 is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support is in place
d. The Customer is responsible for all configuration backups outside of the System without exception.
e. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
f. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook.
g. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier.)
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 Service Charges (as referred to in the Contract).
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 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.

8. Assumptions

a. The relevant System provided under the Contract is covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
b. The relevant System provided under the Contract is in a Valid Supported Configuration at the point of contract start date.
c. All Customer specific pre-requisites have been completed before contract commencement.

9. Pre-requisites

a. Completion of the Enterprise Pre-Launch Questionnaire (ELQ).
b. Platform and where applicable technical tooling inclusive of access to equipment where applicable.
c. Management access for all patching and monitored services.
d. Administrative Access Permissions for ANS Engineers on supported devices.
e. Supplier will grant access to relevant ITSM tool.