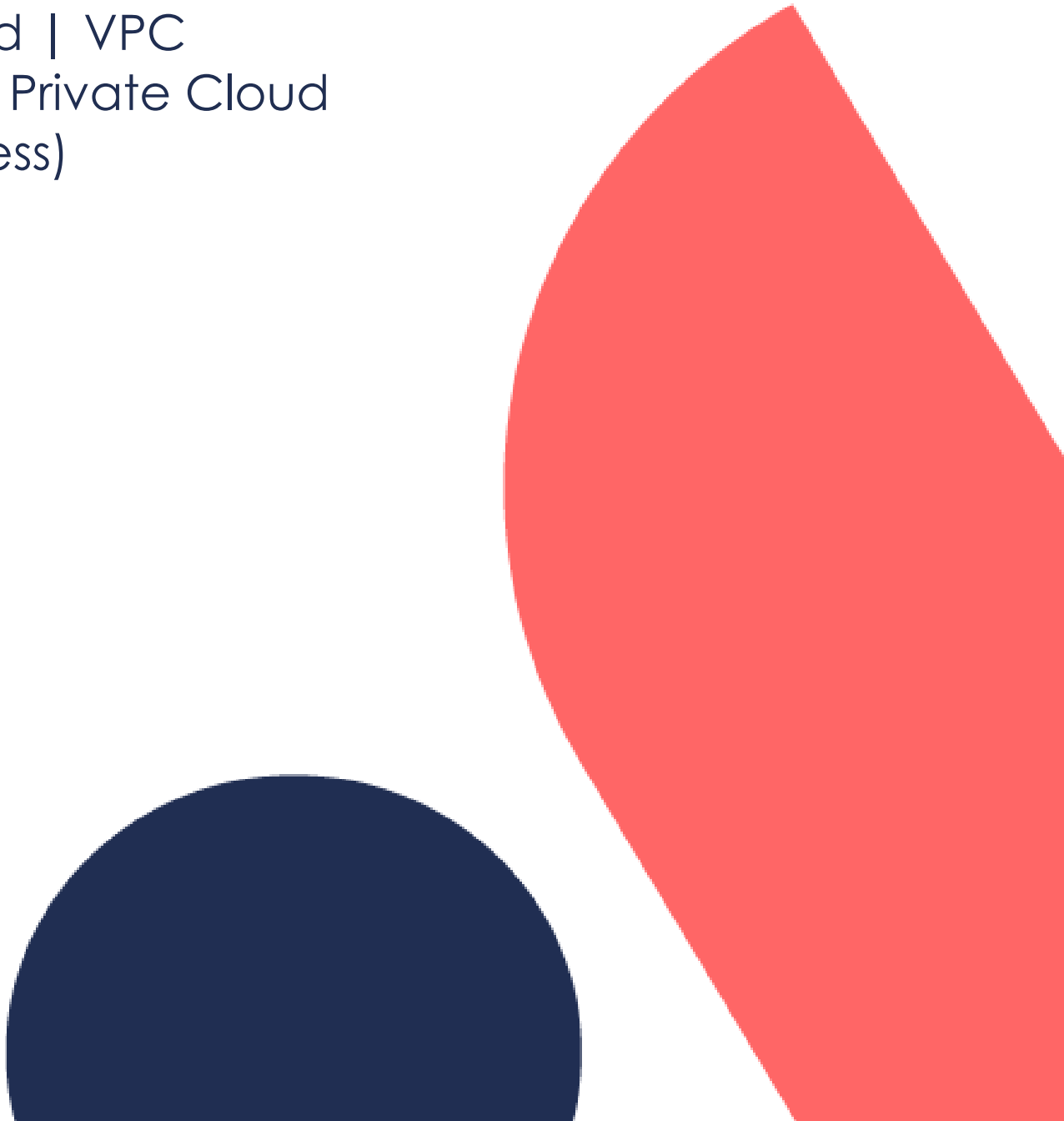
Service Definition

eCloud | VPC
Virtual Private Cloud
(Business)



1. Operational Services

1.1. Terms and Definitions

The following Product Terms apply if the relevant Services are included within your Quotation in the event of a conflict between the Product Terms and the applicable Terms and Conditions, these Product Terms shall prevail, but only to the extent of such conflict. Any capitalised terms used in this document shall have the meanings set out in the applicable Terms and Conditions (save where expressly provided otherwise below) and any additional definitions outlined below shall also apply.

Term	Definition
Normal Business Hours	09:00 – 17:30, Monday to Friday (excluding bank holidays)
Emergency Hours	08:01pm to 07:59am Monday to Sunday including bank holidays.
Working Day	12 Normal Business Hours
24x7	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.
Business Critical Incident	Incidents that cause complete outage or complete failure of systems or services identified by the Customer as crucial to normal business operations.
Change	the addition, modification, or removal of anything that could have a direct or indirect effect on the Service.
Customer Supported Assets	Any resource that is provisioned by the supplier to provide the Customer's eCloud VPC solution.
CSM	non-technical resource provided by the Supplier to facilitate delivery of value to the Customer as part of the Service.
Emergency Change	a Change required in order to resolve or implement a tactical workaround for a P1 incident.
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 the functionality of any part of the system which is provided by the Supplier.
Instance OS	the operating system installed on a virtual machine or cloud instance.
Managed Services Handbook	document provided by the Supplier to provide the Customer with key supporting information regarding the provision of the Services.
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.
Supplier	ANS Group Limited.

System	the functionality related group of elements including hardware and software provided by the Supplier.
Resolution	the criteria for resolution is agreed as part of the impact assessment. When criteria is met, the incident will be marked as resolved and we will contact the Customer to confirm the authority to close the Incident.
Valid Supported Configuration	a configuration of an IT service or component that is formally approved, tested, and supported by the organisation and vendor.
WSUS	Windows Server Update System; a server role in the Windows Server Operating System allowing management and distribution of policy updates.

2. Service Overview

The eCloud VPC (Virtual Private Cloud) combines the benefits of public cloud, such as flexibility, resilience & scalability with the security and simplicity of private cloud. Built on enterprise-grade technology from VMware, Cisco and HPE, the Supplier's cloud platform, eCloud VPC, is tailored to the needs of customers offering a fast and affordable route to the cloud.

The 'Business' service grants the Customer full access to the Supplier's Managed Services Team. This allows the Customer to access support for a broader range of technologies such as Operating Systems, Firewall management, highly available configurations (where purchased) and backup configurations.

3. 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 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 Service Desk for Business Critical system down scenarios (P1) only.	24 x 7
Storage Triage and Troubleshooting	The Supplier investigates and resolves platform incidents relating to storage components.	24 x 7
High Priority Escalation to Vendor	High Priority escalation to vendor for Priority 1 Business Critical faults.	24 x 7
Change Management & Advisory		

OS Patch Management	For Microsoft Servers, if no schedule is agreed the Suppliers default schedule will be applied. The Supplier will update Linux Server installations upon the Client's request working to an agreed process with the Client.	Normal Business Hours
OS Configuration	The Supplier will provide a Web Portal for Configuration Changes on Customer instances for Disk, CPU & RAM.	24 x 7
Software Configuration	The Supplier will update supported applications upon the Client's request working to an agreed process with the Client. This is limited to software installed by the Supplier only.	Normal Business Hours
Backup Setup & Configuration	The Supplier will setup backups where backups have been purchased as part of the service.	Normal Business Hours
Backup Configuration Changes	The Supplier will provide a Web Portal for backup configuration changes.	24 x 7
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.	24 x 7
Monitoring & Event Management		
Monitoring Service	The Supplier will provide the Customer read-only access to monitoring tools, providing uptime and availability monitoring across configured services.	24 x 7
Platform Monitoring	The Supplier will monitor core infrastructure to ensure availability, performance and uptime.	24 x 7
Performance Tuning and Diagnostics	Upon request, the Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customers servers and backups to achieve optimal and consistent performance.	Normal Business Hours
Backup Tooling & Monitoring	The Supplier will monitor, acknowledge and resolve backup failures in line with the SLA where backups have been purchased as part of the service.	Normal Business Hours
Governance, Cost Management & Optimisation		
Cost Reporting	The Supplier shall provide self-service access for the Customer to keep track of spend.	24 x 7
High Availability & Recovery		
HA Configuration	Where a high-availability solution has been deployed the Supplier will configure and manage the availability of the platform infrastructure. However application availability is the responsibility of the Customer.	Normal Business Hours
Failover Management & Recovery	Where a high-availability solution has been deployed, the Supplier will help manage failover during P1 incidents.	24 x 7

Protect & Recover		
High Priority Backup Restores	Where backups have been purchased as part of the service, the Supplier will commit to backup restores of customer supported assets when a Priority 1 (P1) incident is raised with the Supplier.	24 x 7
Backup & Recovery	Where backups are purchased as part of the service, the Supplier will setup backups and recover from backups on request.	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.	Normal Business Hours
Antivirus	Where a Security Product is licensed and purchased as part of the eCloud VPC solution, the Supplier will deploy and manage required policies.	Normal Business Hours
Service Operations		
Customer Portal Access	Customer access to ANS Glass providing visibility of all Service-related tickets, billing information, and self-service access (where available).	24 x 7
Account Management	The Supplier shall provide an account management function for the Customer and where applicable to the Service a CSM will be aligned to the account. This will be confirmed during agreement of the Quotation and Terms.	Normal Business Hours
Emergency Changes	Following a Business Critical Incident, the Supplier will implement Emergency Changes within the scope of the Service.	24 x 7
Root Cause Analysis	Applicable to P1 Incidents only, following the successful resolution of the Incident. In the case of reoccurring incidents, further analysis may be undertaken, and Service Disruption Report created.	Normal Business Hours
Physical Asset Protection		
Infrastructure Services	The Supplier will manage the infrastructure as a service, including software and firmware versions as per the vendors advice.	24 x 7
Hardware – Non-Business Critical Faults	The Supplier provides all physical hardware in N+1 configuration or highly available therefore 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 Business Critical system down scenarios (P1).	24 x 7

4. Incident & Request 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 P5. Each category of classification has an SLA for Response time and a Resolution target.

4.1. Incident Priority Table:

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	P5	P4	P3

4.2. Incident & Request Response

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 employee responds whether via an email, ANS Glass update, telephone call or in person. P1 incidents must be telephoned in to the Supplier. For a detailed process flow, please refer to the Managed Services Handbook.

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

From the time of Response until resolution, updates shall be provided to the named contacts on the Customer's account through ANS Glass at such frequencies as set out in the table above.

The SLA clock will not commence until the appropriate set of information to allow investigation has been received. The SLA clock will be stopped during periods where the incident is back with the Customer or where an action is required outside of the Supplier's team.

There is no limit on the number of support requests, but excessive usage (beyond Acceptable Use Policy) will be investigated by the Supplier and future requests may be chargeable.

5. Service Levels, Key Performance Indicators and Service Credits

Service Credits are calculated as a percentage of the monthly Charges and in any event shall not exceed 10% of the monthly Charge in the month that the Service Credit arose.

Incident Category	Service Level Target	Minimum Service Level	Service Credits
P1	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.	100%	1st Incident missed response time – 5% Service Credit
P2	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	100% of Incidents responded to within 4 Normal Business Hours.	None	No Service Credit
P4	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5	100% of Incidents responded to within 2 Working Days.	None	No Service Credit

6. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the applicable 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 making changes to the System.
d. Any issues caused where the software provided by the Customer does not conform to the design and/or specification requirements agreed in writing with the Supplier. This shall include the requirement for the Customer to have an ANS-provided firewall device as part of the solution design.
e. The availability of any application programming interface (API) written and provided by the Supplier as part of the Service.
f. End User or 1st line support.

g. Technical Advice to any persons not listed as a named contact on the Customer's account.
h. Where Service Credits are directly associated or linked to a minimum service level percentage, there must be a minimum of 4 tickets, or the service credit shall be excluded.
i. Normal Changes requiring more than 2 hours of implementation time are excluded from the Service and may be subject to Additional Service Charges.
j. Changes outside of Normal Business Hours may be subject to additional Charges.
k. 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. Where required, the Customer shall make available appropriately skilled employees 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 the System (regardless of perceived impact)
c. 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 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.
f. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the System, including environmental changes.
g. 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.
h. The Customer must be able to provide the Supplier with accurate application and services information for the Supplier to successfully on-board the service.
i. The Customer is responsible for applications not installed by the Supplier.
j. The Customer is responsible for the security and integrity of the operating system and application stack unless purchased as an additional service.

8. Assumptions

a. All Customer Supported Assets within this contract are covered by a valid software maintenance and support agreement in line with applicable Service Levels.
b. All Customer Supported Assets are in a Valid Supported Configuration at commencement of the Agreement.
c. All Customer specific pre-requisites have been completed before commencement of the contract.
d. Additional services can be purchased in conjunction, i.e. EDR,, Backups, and panel licenses.

9. Pre-Requisites

To onboard and deliver te Services optimally, certain pre-requisites must be met. The Supplier's delivery team will work closely with the Customer on the pre-requsites.

These pre-requisites are:

1. Administrative Access Permissions for Supplier Engineers on Instance OS and supported applications where relevant.
2. Approved Statement of Work/Pre-Launch Questionnaire.
3. The Supplier will grant access to the Customer to ANS Glass

10. Responsibility Matrix (RACI)

RACI: R=Responsible | A=Accountable | C=Consulted | I=Informed			
Activity	**ANS**	**Client**	**Comments**
Creation/Deletion of VPC	R/I	R/C	Where a Managed Service has been purchased, there is shared responsibility via the sales and launch process or through the ANS Glass. Otherwise, the responsibility is with the Supplier for the initial launch of VPC, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.
Creation/Deletion of Networks	R/I	R/C	Where a Managed Service has been purchased, there is shared responsibility via the sales and launch process or through ANS Glass. Otherwise, the responsibility is with the Supplier for the initial launch of VPC, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.
Creation/Deletion of Routers	R/I	R/C	Where a Managed Service has been purchased, there is shared responsibility via the sales and launch process or through ANS Glass. Otherwise, the responsibility is with the Supplier for the initial launch of VPC, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.

Creation/Deletion Private Hosts	R/I	R/C	Where a Managed Service has been purchased, there is shared responsibility via the sales and launch process or through ANS Glass. Otherwise, the responsibility is with the Supplier for the initial launch of VPC, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.
Creation/Deletion of Instances	R/I	R/C	For supported customers shared responsibility based on self-creation through ANS Glass or through launch process. For unsupported customers the initial launch may be the Supplier's responsibility because of automated launch, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.
Activity	**ANS**	**Client**	**Comments**
Creation/Deletion of Volumes	R/I	R/C	Where a Managed Service has been purchased, there is shared responsibility via the sales and launch process or through ANS Glass. Otherwise, the responsibility is with the Supplier for the initial launch of VPC, subsequent to this additional capacity is the responsibility of the Customer. When the Customer has terminated the Services or upon expiry of the Agreement, the Customer is responsible for deleting the resources in use via ANS Glass. Should these not be deleted such resources will be chargeable at the eCloud VPC PAYG rate.
Installation of Supported Software	R/I	R/C	The Supplier will support software installed by the Supplier.
Installation of 3rd party software	I	R	
Resource Management			
Instance CPU Increase/Decrease	I	R	
Instance Memory Increase/Decrease	I	R	
Instance local volume Increase/Decrease	I	R	
Shared volume Increase/Decrease	I	R	

IP creation/deletion/assignment	I	R	
Private Host CPU Spec Change	I	R	
Private Host Memory Spec Change	I	R	
ACL creation/deletion	I	R	
Storage IOPS Increase/Decrease	I	R	
Performance management			
Infrastructure Storage Performance	R	I	
Infrastructure Network Performance	R	I	
Infrastructure Compute Performance	R	I	
VM Storage Performance	R/C	R/C	Where a Managed Service has been purchased, responsibility for VM performance is shared, the Supplier assumes responsibility up to and including the OS layer. Application interaction with the underlying infrastructure is therefore the Customer's responsibility.
Activity	**ANS**	**Client**	**Comments**
VM Network Performance	R/C	R/C	Where a Managed Service has been purchased, responsibility for VM performance is shared, the Supplier assumes responsibility up to and including the OS layer. Application interaction with the underlying infrastructure is therefore the Customer's responsibility
VM Compute performance	R/C	R/C	Where a Managed Service has been purchased, responsibility for VM performance is shared, the Supplier assumes responsibility up to and including the OS layer. Application interaction with the underlying infrastructure is therefore the Customer's responsibility.
Application Performance	I	R	
Storage Patching	R		
Public Host Patching	R		
Private Host Patching	R	C/I	Private Customers will be consulted on underlying patching prior to implementation except in emergency situations where they will always be informed before the work begins.
Management Patching	R		

Network Patching	R		
VM Patching	I	R	
Infrastructure monitoring	R		
Public hardware failures	R		
Private Hardware failures	R	I/C	Private Customers will be consulted on underlying hardware changes prior to implementation except in emergency situations where they will always be informed before the work begins.
Infrastructure Security	R		
Solution Security	C	R/C	The Supplier assumes responsibility for the security of the underlying infrastructure, it is the Customer's responsibility to ensure the application stack and its interaction with the Supplier's infrastructure are secure.