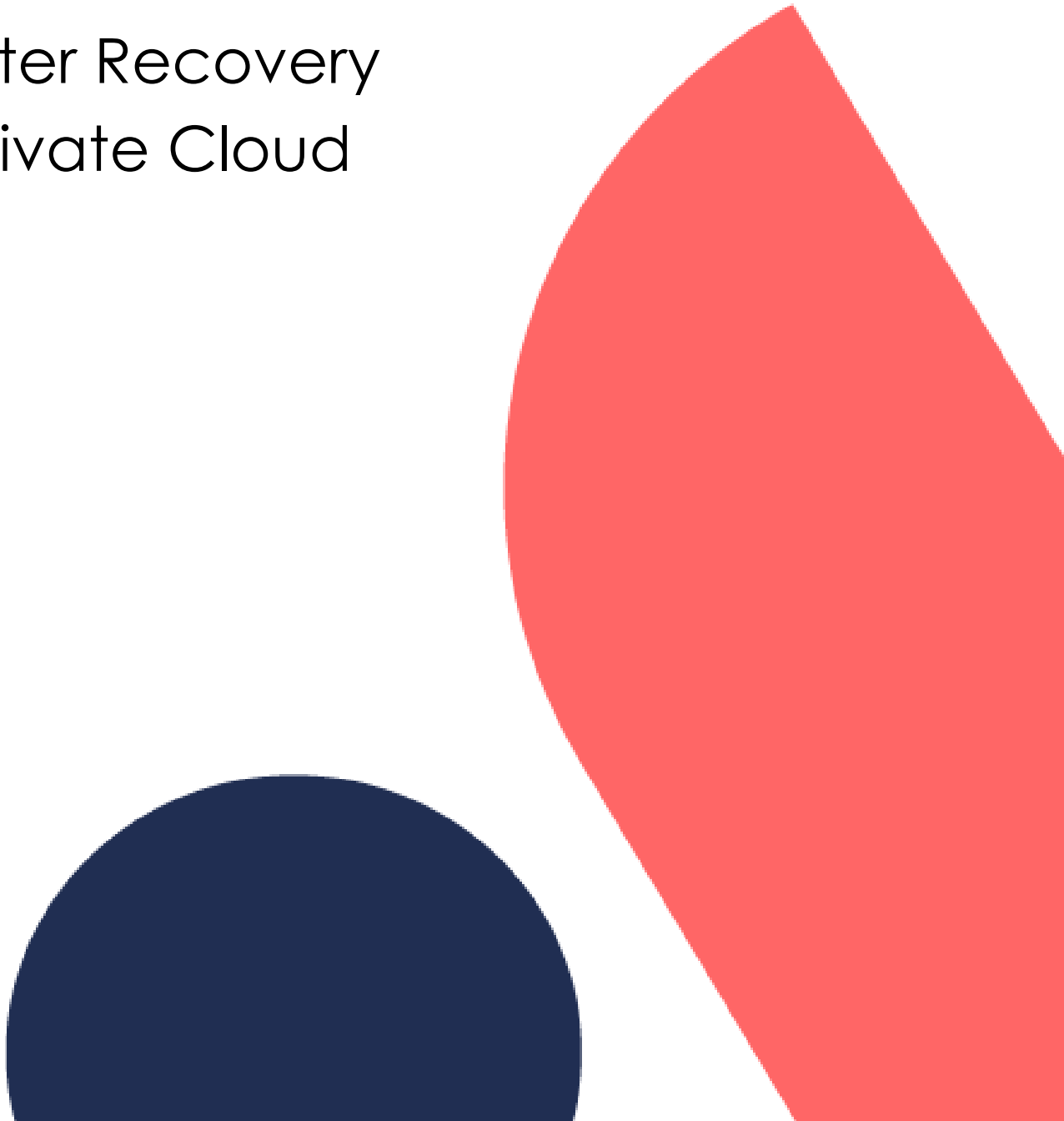
Service Definition

Disaster Recovery for Private Cloud



1. Operational Services

The definitions used in the Terms shall have the same meaning when used in this Service Definition. The following additional terms used in this Service Definition are defined as follows:

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.
ANS Glass	The portal where the Customer can log/view Service-related tickets, alerts and performance dashboards and raise Incidents.
Business Critical Incident	Incidents that cause complete outage or 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.
Change Management Process	The Supplier's structured approach to managing Changes.
Customer Supported Assets	Any resource that has been assigned with a Recovery Plan within the Disaster Recovery Management Portal that is intended to be replicated into the failover site.
Disaster Recovery Document of understanding	Contains the process for failover and failback and documents the assets that are protected and that are in scope of the protection schedule.
Disaster Recovery Management Portal	Management Portal for the Disaster Recovery tooling provided by the Supplier.
Emergency Change	A Change required to resolve or implement a tactical workaround for a P1 incident.
Escalation Manager	Technical escalation point, typically a Supplier employee.
Failover Test	A controlled exercise used to verify a system, application or network can successfully switch from its primary environment to a backup or secondary environment when the primary system becomes unavailable due to a failure, maintenance, or other disruption.
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 which is provided by the Supplier.
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 or Emergency Change. It goes through the Change Management Process, including assessment, authorisation and scheduling.
Recovery Plan	A DR schedule and failover plan within the DR software
Request	A pre-defined, pre-authorised request from a user for something to be provided.
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 the Supplier will contact the Customer to confirm the authority to close the incident.
RPO	Recovery Point Objective; defines how far back in time your data recovery efforts must go to restore operations after a failure.
RTO	Recovery Time Objective; defines maximum acceptable duration of time for a system, application, or business process can be unavailable
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 and/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 Management Review	Regular meeting delivered by the Supplier focused on performance and value of the Managed Services contracted.
Standard Changes	A pre-authorised Change that is low risk and follows a documented process for implementation.
Support Requirement	A formally logged request or incident initiated by the Customer, that requires technical investigation, remediation, or advisory action by the Supplier. A Support Requirement is considered to fall within the scope of the Supplier's responsibility when the root cause is attributable to the DR software provider's services.
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 organisation and vendor.

2. Operations Baseline

Service	Service Description	Service Hours
Incident Management		
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and portal 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 Service Desk for critical system down scenarios (P1) only.	24 x 7
High Priority Recovery	The Supplier will commit to recovery of Customer Supported Assets upon a Priority 1 (P1) Incident being raised with the Supplier requesting failover and a support ticket raised by the Customer.	24 x 7
DR Failback	The Supplier will decide in partnership with the Customer on whether a DR failback is required. In the event failback of DR is agreed, the Supplier commits to DR failback operations upon notification and discussion with the Customer and agreement of a failback plan.	Normal Business Hours
Change Management & Advisory		
Protection Reporting and Ops Advisory	The Supplier will provide reporting to highlight any virtual machines within the estate that are not protected by the Services.	Normal Business Hours
Change Guidance & Architecture Validation for Disaster Recovery	The Supplier provides expert access to Change advisory for: 1. Disaster Recovery architecture & configuration 2. Disaster Recovery policy validation 3. Disaster Recovery design	Normal Business Hours
DR Setup & Configuration	The Supplier will setup and configure new Recovery Plans via a normal Change to standard specifications and then customise settings to suit Customer requirements	Normal Business Hours
Patch Management	The Supplier will ensure the backend DR infrastructure will receive updates patches as according to the Supplier's patching schedule.	Normal Business Hours

High Availability & Recovery		
Recovery Plans	The Supplier will setup Recovery Plans where requested and help recover / failover where requested.	Normal Business Hours
Test Recovery Plans	The Supplier will commit to testing Recovery Plans of Customer Supported Assets annually upon a Normal Change being raised.	Normal Business Hours
Platform Monitoring & Event Management		
Platform Monitoring	1. DR Infrastructure monitoring 2. Performance monitoring 3. Capacity monitoring	24 x 7
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.	24 x 7
Performance Tuning and Diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customer's replication achieve better and more consistent performance. Additional license fees may apply.	Normal Business Hours
DR Tooling & Monitoring	The Supplier will monitor overrunning DR replication jobs and failures including remediation via rescheduling.	Normal Business Hours
Protect & Recover **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
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
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 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 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

3. Service Overview

ANS Private Cloud Disaster Recovery Services provides Virtual Machine (VM) replication to secondary compute and storage resource pools located within a secondary data centre. Private Cloud Disaster Recovery Services are used to provide geo-location protection services for Supplier Private Cloud solutions and as such is not a standalone product.

Disaster Recovery Services manage the replication of VMs, asynchronous replication occurs hourly with 24 restore points available for service restoration, with the lowest RPO being one hour. Failover to the DR site is a manual process and will require network reconfiguration as different external IP addresses will be used to those in the live site. Either the entire VM estate can be replicated or a subset of the estate (i.e. production VMs only) which should be clearly defined in a Disaster Recovery Document of Understanding. DNS and VPN endpoints will need to be repointed after failover has occurred.

The configuration of the preferred technical solution will be specific to the Customer needs as outlined in the SOW and the relevant level of support as defined by this document.

4. Incident Management

Incidents have a wide scope and can fall into different classification and prioritisation levels.

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.

4.1. 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	P5	P4	P3

4.2. 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 a Supplier employee responds whether via an email, ANS Glass 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 Incident Resolution.

The 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 via 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's team.

Priority	Response SLA	Specialist Review	Escalation Manager	Notification Frequency	Target Resolution KPI
P1	30 Minutes	2 Hours	Immediate	Hourly Email	4 hours
P2	1 Hour	4 Hours	1 Day	GLASS Portal	2 Days
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

5. Service Levels & Key Performance Indicators

Category	Service Level Target
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.
P4 Incidents	100% of Incidents responded to within 1 Working Day.
P5 Incidents	100% of Incidents responded to within 2 Working Days.
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution.

6. Responsibility Matrix

Activity	Supplier	Customer	Comments
Creation of Disaster Recovery Document of Understanding	✓	✓	The Supplier will support in the creation of the Disaster Recovery Document of Understanding in collaboration with the Customer during the initial delivery of the Service.
Maintenance of Disaster Recovery Document of Understanding		✓	
Set up of DR environment	✓		
Set up of initial Recovery Plans	✓		
Maintenance of the Recovery Plans		✓	The Customer is responsible for maintaining and managing their Recovery

			Plans within the Disaster Recover management portal.
Authorising and requesting failover or failback		✓	Failover will only be initiated upon Customer request
Performing failover and failback		✓	The Customer can initiate failover within the DR management portal or request support to initiate failover
Management of Resources within the failover site		✓	The Customer has the same responsibilities to manage the resources within the failover site as in the service supporting the primary site.
DNS update / VPN failover when in failover		✓	
Annual Failover Test upon request	✓		
Disaster Recovery systems Performance	✓		
Failover Site Infrastructure Performance	✓		

7. 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 Disaster Recovery Document of Understanding resulting in impact to the Customer Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Demarcation Zone resulting in impact to the Customer Supported Assets.
c. Issues resulting from unauthorised access by the Customer of Customer Supported Assets.
d. End User or 1st line support.
e. Technical Advice to any persons not listed as a named contact on the Customer's account.
f. Failure to meet SLA due to local environmental factors such as power and cooling.
g. Patching of Customer Supported Assets that do not comply with vendor best practices and configurations.

8. 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 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 shall provide full physical access to all Customer Supported Assets at Customer premises if/when required.
e. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide adequate access to allow investigations to proceed.
f. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support in place.
g. The Customer is responsible for completing a Change Request in accordance with the Supplier's Change Management Process.
h. The Customer shall ensure that all relevant Customer employees have access to and have read the Managed Services Handbook.
i. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier).
j. 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.
k. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
l. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets. Any asset that has been moved without notification to the Supplier will be subject to Additional Service Charges.
m. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.
n. 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.
o. The Customer is responsible for the sign-off of each patch cycle ensuring User Acceptance Testing (UAT) has been completed. Without feedback the UAT process is assumed accepted by the Customer and patching will progress by the Supplier.
p. The Customer is responsible for requesting failover and failback.
q. The Customer is responsible for any additional costs consumed during failover.
r. The Customer is responsible for maintaining and managing their Disaster Recovery Document of Understanding and communicating changes back to the Supplier.
s. The Customer is responsible for maintaining and managing their Recovery Plans within the Disaster Recovery Management Portal.

9. Assumptions

a. The relevant System provided under the Contract is covered by a valid software maintenance and support agreement in line with applicable Service Levels.
b. The relevant System provided under the Contract is in a Valid Supported Configuration at the Commencement Date.
c. All Customer specific pre-requisites have been completed before the Commencement Date.
d. The Customer will provide resource to work with the Supplier to on-board the Service and assist with maintenance tasks as required.
e. Any requested support for maintenance of the Disaster Recovery Document of Understanding will be delivered via Professional Services and will incur further charges.
f. Work done by the Supplier on the Customer's 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. Support of applications is only up to the OS layer that is part of the solution.
i. ANS will support in the creation of the Disaster Recovery Document of Understanding in collaboration with the Customer during the initial delivery of the Service.

10. Pre-requisites

a. Completion of the Supplier's Enterprise Pre-Launch Questionnaire (ELQ).
b. Management access for all patching and monitored services.
c. Administrative relevant access permissions for the Supplier's engineers on supported devices where required.
d. Supplier will grant access to ANS Glass.
e. All Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with applicable Service Levels.
f. All Customer Supported Assets are in a Valid Supported Configuration at the Commencement Date.
g. Customer has an enhanced level of support with the supplier for the Cloud Solution that this Service is being provided for.