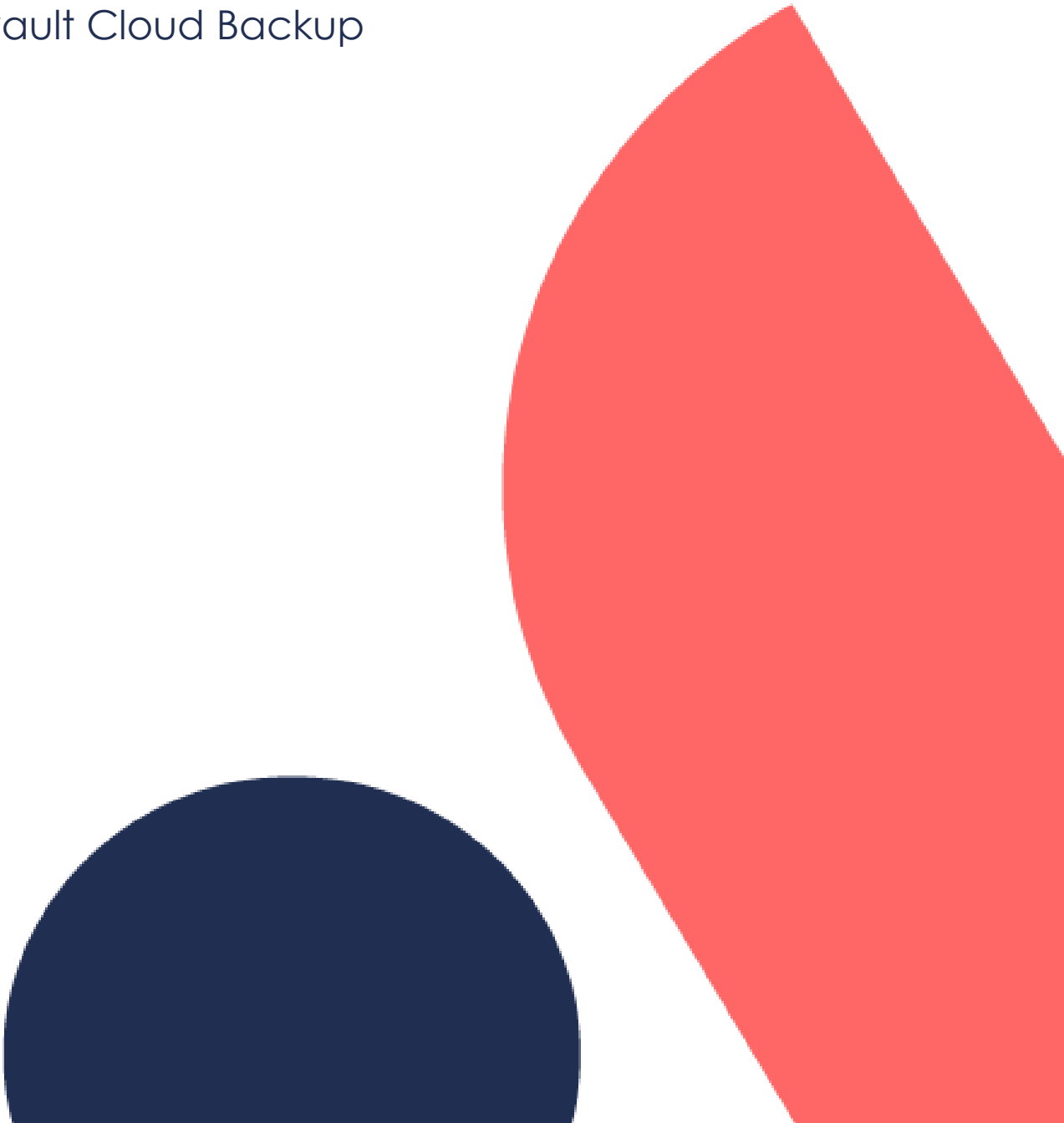
Service Definition

Commvault Cloud Backup



1. Service Overview

The service provides a centrally managed platform for multiple data sources and is backed by governance and continual improvement, providing assurance of the solution's effectiveness during an event when a restore is required.

The configuration of the preferred technical solution inclusive of backup storage location will be specific to the Customer needs as outlined in the SOW and the relevant level of support as defined in this Service Definition. The scope of this Service will be determined by the technology and service selection at the point of sale.

2. Operational Services

2.1. Terms and definitions

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:

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.
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.
Change Request Form	Template that allows the Customer to submit requested Changes to the Supplier as part of the Change Management Process.
Co-Managed	The Cloud Service Provider and the Customer share the responsibility of managing the solution. This hybrid approach allows the Customer to remain in control over certain

	aspects of the solution, while outsourcing more complex or resource intensive tasks to 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.
Emergency Change	A change required in order to resolve or implement a tactical workaround for a P1 incident.
Escalation Manager	Technical escalation point, typically a Supplier employee.
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.
Request	pre-defined, pre-authorised request from a user for something to be provided.
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, 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.
System	The functionally related group of elements including hardware and software provided by the Supplier.
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.
Root Cause Analysis	A process used to identify the underlying cause(s) of Incidents or problems.

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 provider's services.
Valid Supported Configuration	A configuration of an IT service or component that is formally approved, tested, and supported by the Supplier and vendor

2.2. Operations Baseline

Service	Service Description	Service Hours
Incident Management		
Service Desk - Non Business Critical Faults	The Supplier provides access via ANS Glass, 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		
Backup Agent Configuration	Where an agent/backup gateway/media agent is deployed, the Supplier will rollout updates on an agreed schedule with the customer.	Normal Business Hours
Backup Setup & Configuration via Self-Service Portal	Backup requirements to be configured during the term of the Service 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

	The Supplier will provide support upon Customer request.	
Platform Monitoring & Event Management		
Backup Success Monitoring	The Supplier will monitor backup health and will provide alerting for failure using pre-defined and appropriate thresholds to alert both support teams and the Customer of developing issues.	24 x 7
Performance Tuning and Diagnostics	Upon request, the Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customer's solution and backups to achieve better and more consistent performance.	Normal Business Hours
Failure & Remediation	The Supplier will monitor overrunning backup jobs and failures including remediation via rescheduled backups.	Normal Business Hours
Protect & Recover		
Backup & Recovery	The Supplier will setup backups where requested by the Customer and help restore from backup where requested. Access to a portal will also be provided for the self-service management of backups, offering the ability to create new backups and restore backups.	Normal Business Hours
High Priority Backup Restores	In the event that the Customer is not able to restore a high priority backup, the Supplier will use reasonably endeavours to support the Customer with 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 reasonably endeavour to test backup restores of Customer supported assets upon an agreed schedule being submitted by the Customer to the Supplier. To initiate this, the Customer must raise a ticket with 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. The ANS Glass portal also facilitates access to configure and manage backup provisioning and management of resources.	24 x 7
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a Platform P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken via the Problem Management process to identify the underlying cause.	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.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 x 7
Customer Success		
Service Reviews	Service Management Review (SMR) Reports will be distributed at regular intervals. The SMR Report will cover the previous period.	Normal Business Hours

3. Incident Management

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 (as defined below) and a Resolution target.

3.1. 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

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's 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 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 account by email or ANS Glass 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 the Supplier's team.

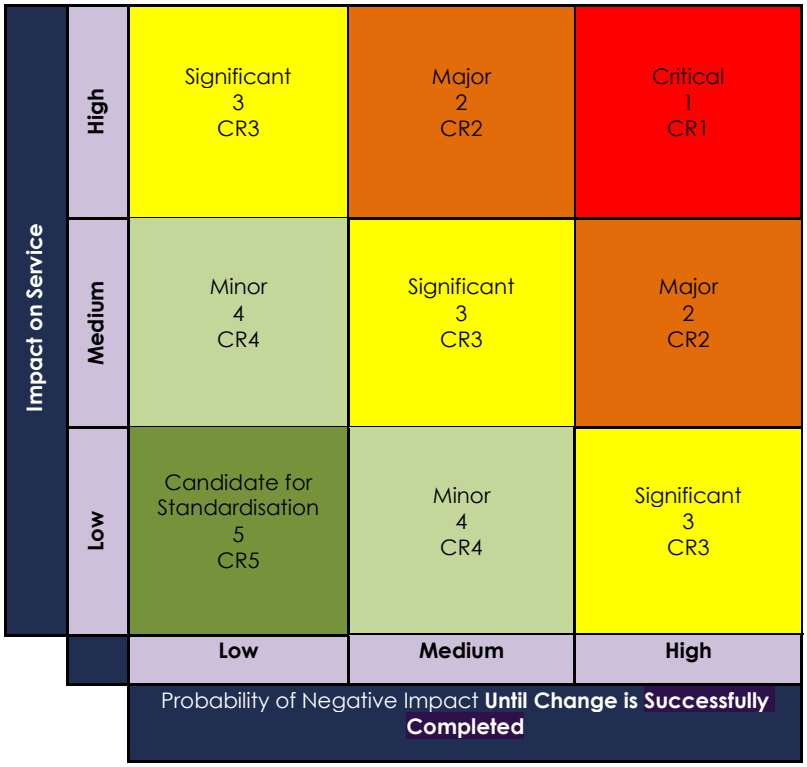
Priority	Response SLA	Specialist Review	Escalation Manager	Notification Frequency	Target Resolution KPI
P1	30 Minutes	2 Hours	Immediate	Hourly Email	4 hours
P2	1 Hour	4 Hours	1 Day	GLASS Portal	2 Days
P3	4 Hours	2 Days	4 Days	GLASS Portal	10 Days
P4	1 Day	Never	Never	GLASS Portal	30 Days
P5	2 Days	Never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

3.3. Change Management

All Changes require a Change Request Form to be completed on ANS Glass Portal 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) and/or a major Security Incident where the Supplier deems appropriate.

Change RISK Matrix



Change implementation target 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 Service within the scope of the Contract will be completed by the Supplier at no additional cost.

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

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. API platform automation and ANS Glass access is not within scope of Service Credits. 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.

5. Responsibility Matrix

Responsibilities	ANS	Customer
In Service Configuration	✔	✔
Failure Monitoring	✔	
In service Restores	✔	✔

6. 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 the Supplier 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 resulting from unauthorised access as a result of the Customer's actions
e. Issues created by the Customer making changes to the solution that impacts the ability of the Supplier to deliver the service
f. 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.
g. Any issues caused by negligence on the part of the Customer, its employees, servants or agents.
h. The availability of any Application Programming Interface (API) written and provided by the Supplier as part of the Services.
i. End User or 1st line support.
j. Technical advice to discuss account specific details including technical advice to any persons not listed as a named contact on the Customer's account.
k. Emergency Changes that are not a direct output of a priority 1 Incident may be subject to Additional Service Charges.
l. 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
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. Failure to meet SLA due to Public Cloud provider or Backup SaaS Provider outages or local environment factors such as power and cooling
o. Normal changes requiring more that 2 hours of implementation time are excluded from the Service and will be subject to Additional Service Charges
p. Installation and/or configuration of the backup agents on any servers that are not supported by the Supplier.
q. Project Changes (Normal CR6) are excluded from the Service and will be subject to Additional Service Charges. Project Changes are recorded within ANS Glass for informational and approval purposes only

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:
    - Affected Services
      Business impact
      Number & type of users affected
      Recent changes on Customer Supported Assets (regardless of perceived impact)
    - 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 shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed.
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 Supplier's 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 client side where relevant.
h. The Customer shall ensure 24x7x365 availability of a suitable escalation contact on the Customer account 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 P1 Business-Critical Incidents raised via email.
k. 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 and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to ANS will be subject to Additional Service Charges
l. 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.
m. The Customer is responsible for applications not installed by the Supplier.
n. The Customer is responsible for the security and integrity of the operating system and application stack unless support is purchased.
o. The Customer is responsible for 1st line restoration of files and folders.
p. Where Managed OS has not been purchased, The Customer is responsible for deployment of agents to servers, applications or virtual infrastructure
q. The Customer shall ensure that all relevant Customer employees have access to and have read the Managed Services Handbook.

8. Assumptions

a. All Customer data that is being backed up is a part of a Co-Managed Service with the Supplier
b. All Customer Supported Assets and production AWS and Azure Accounts within the Customer Supported Assets within the Contract are covered by a valid software maintenance and support agreement in line with the applicable Service levels.
c. The relevant System provided under the Contract is covered by a valid software maintenance and support agreement in line with applicable Service levels.
d. The relevant System provided under the Contract is in a Valid Supported Configuration at the Commencement Date.
e. All Customer specific pre-requisites have been completed before the Commencement Date. The Customer will provide resource to work with the Supplier to on-board the service and assist with maintenance tasks as required.
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. Terms for any ancillary support services provided by the Supplier to the Customer would not be considered part of this Service
i. Azure tenant available for Microsoft Azure BLOB storage

9. Pre-requisites

a. The environments/solutions that are being backup up must be supported by a Supplier Managed Service
b. Completion of the Supplier's "Enterprise Pre-Launch Questionnaire" (ELQ).
c. Administrative Relevant Access Permissions for Supplier's engineers on supported devices where required.
d. Supplier will grant access to ANS Glass.
e. All Customer Supported Assets within the 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. Deployment of ANS monitoring and backup tooling.