SYNAPSE360

Managed Service Definition

Cyber Recovery as a Service

MSD-CRS-01

Contents

Document Purpose

Internal

- To enable Synapse 360 or agent sales & account management to accurately convey the available managed service to our customers
- To provide the basis for marketing teams to create truly representative and inspiring messaging to introduce our managed service to new audiences
- To provide the basis for the NOC and contracts team to scope and provide the best quality managed service
- To enable the Service Delivery Manager (SDM) to evolve the managed service to continuously improve the customer experience

External

- To convey to customers what the managed service will deliver and when
- To eliminate ambiguity of the managed service and set accurate expectations around service levels and deliverables

Document control

Status:	Internal for Review
Issue Version:	1.1
Date of Issue:	

Amendment Summary

Issue	Date	Commentary	Initials
1.0	14/04/20	Initial draft document	JP
1.1	01/12/22	Branding Update	CK
1.2			

1 Managed Service Overview

Synapse 360's Cyber Recovery as a Service (CRS) gives customers the assurance that they can quickly recover business services in the event of a cyber security breach.

CRS copies selected backup data that is considered critical to the business to a secure, resilient and isolated environment (the vault) within their own datacentres or one of Synapse 360's datacentres. Access to the vault is highly restricted preventing internal threats from physically affecting the service.
Replication of the backup data happens during a random window in which the "air gap" is opened.
Once the backup is completed the air-gap closes and the data is locked for compliance. It is then analysed by CyberSense which can detect an exploit in the early stages and identify the best clean copy to restore from. Recovery testing servers and storage are also held in the vault which are used for testing by Synapse360 twice a year.

Key Facts
A managed service to control, monitor and maintain the cyber recovery capabilities for customers. Synapse 360 will create and amend backup and recovery jobs, protection groups, perform test failovers restores, and implement major release software updates. ▪ 24x7 recovery management from the Synapse 360 Network Operation Centre (NOC) ▪ Synapse 360 take protection ownership of the Cyber Recovery data and include a managed Avamar Virtual Edition to protect this data both day to day and for Cyber Recovery ▪ Built on Dell Cyber Recovery, Avamar and Data Domain ▪ Recovery infrastructure is built on PowerEdge and Dell EMC Powerstore ▪ OPEX model includes licensing, platform and managed services with support ▪ Cyber Recovery testing twice annually and Cyber Recovery support is included ▪ ISO 20000 accredited Synapse 360 NOC ▪ All data can be encrypted in transit and at rest ▪ Choose where your data resides: a Synapse 360 UK based data centre, or on-premise / co-location ▪ Major software version upgrades are included where they are available via a valid license agreement and recommended by the Synapse 360 CRS team – this will occur during vault visits (twice annually)

Vendor Terms
All hardware and software that is involved in the service must be under a current vendor support agreement for the CRS version. The service level from Synapse 360 will immediately default to 'best endeavours' where vendor support has expired.

Ordering Information
The CRS service is currently available for customers running VMware vSphere and/or Microsoft Hyper-V software. **The service is constructed in a modular format to protect Synapse Managed Services in a Dell controlled sale and allow Synapse to bolt Cyber Recovery services to existing customer hardware.**

- Synapse 360 Cyber Recovery Complete Service– For customers who wish to have a predictable cost model for cyber recovery. All hardware, software and managed services are provided as a single monthly cost.

- Synapse 360 Cyber Recovery Managed Service Only – for customers who want to own all the relevant hardware and software but want to benefit from Synapse 360 Managed Services. This is a service only contract. Synapse 360 will design and implement the solution prior to the day to day management.

2 Service Scope

Synapse 360 strives to delight customers and provide the best in class managed services every day. Please review this section to understand the components of the service.

- Service Package – Defines the service and options.
- Preparation Services – Activities that will be carried out during acceptance or on-boarding.
- Managed Service Level Comparison – The included service elements provided from within the Synapse 360 NOC, hardware and licenses.
- Service Platform Components – The software, hardware and Cloud components provided within the CRS product.

Services outside of scope will require prior agreement and will be charged for.

2.1 Service Package

Objective	To provide a remote Cyber Recovery and recovery orchestration solution that advances traditional on-line backup options with the security required for an air gapped data protection vault.
Supported From	All support and management is provided remotely from the secure ISO 20000 accredited Synapse 360 Network Operations Centre (NOC). No work is ever outsourced. Vendors may, from time to time, provide remote support for hardware or software faults.
Access and Security	The Synapse 360 NOC requires remote access to the Primary Avamar system which will be provisioned during the on-boarding. Remote access into the vault is strictly forbidden. Only Data Domain replication traffic is permitted into the vault. Our networking team will work with you to ensure a secure and trusted connection is only available from inside our ISO accredited NOC to the Avamar system. Connection will be via encrypted site-to-site VPN.
Support Level	Monitoring, provision of remediation advice and instruction, job creation and modification (change request), restores (change request) either to original or alternative location in the same digital location. Critical 27x365x7 Response 2 hours. The CRS managed service involves the cyber recovery components only.
Engagement	▪ Monitor and manage scheduled backup jobs ▪ Provide quarterly updates with backup success rates, high level data insight, data growth, recurrent issues, recommendations, breaches ▪ Receive change requests form the customer to amend, create or delete backup jobs ▪ Receive change requests from the customer to perform test, overwrite or alternative location restores ▪ Customers can raise ticket requests via email or phone and monitor directly using the Synapse 360 Autotask portal
Supported Products	The CRS managed service includes or supports the following products: ▪ Dell EMC Integrated Data Protection Appliance (IDPA) ▪ Dell EMC Data Domain (Physical only)

	▪ Dell EMC Avamar ▪ Dell EMC Networker ▪ Dell EMC PowerEdge, PowerSwitch ▪ Dell EMC Unity XT ▪ SonicWall NSA Customers with alternative backup products can continue to use these products for non-Cyber protected data.
Service Boundary[1]	The Synapse 360 CRS managed service covers all aspects of the supported Cyber Recover infrastructure, while the customer is responsible for the production infrastructure, data integrity, virtual machines, operating systems, agents (including but not limited to xVSS, VMware Agent)
Infrastructure Requirements	Delivery of the CRS will require the customer to provide some or all of the following: ▪ Data Centre facility and connectivity into the vault (1GbE minimum) ▪ Resources for Avamar Virtual Edition Proxy; 4GB RAM, 30GB HDD, 1 vCPU (x2) AVE: 16GB RAM, 200GB HDD / 3TB Thin Provisioned, 2 x vCPU, 1 x Virtual
Review and Update	Our Customers are our most important asset alongside our own experts and it is important for us to build post sales relationships whist demonstrating value with our managed services. Customers will interact with the Synapse 360 NOC, and in addition quarterly remote Teams updates are provided to review the service and discuss any recommendations or remediation.
Out of Scope	▪ The monitoring of customers on-premise infrastructure, applications and services for outages ▪ The protection of operating systems not included in the A.3: Protected Operating Systems section

[1] To illustrate the service boundary a VM workload backup may fail because of a pre-existing snapshot or snap that requires attention within the VMware infrastructure. The Synapse 360 NOC will monitor the backup failure and make recommendation to the customer of what remediation actions are required. Once the customer has performed the actions they may request that the backup runs as usual on the next schedule, or that the Synapse 360 NOC creates a manual protection task to run at another time.

2.2 Preparation Services

Managed service success is derived through trust, exceeding expectation, along with the skills and service (values) of the individuals and service provider. In order to demonstrate the knowledge, experience and skill of Synapse 360 the following services are provided free of charge (FOC) prior to contract:

- Assessment and sizing – Using our toolset to assess virtual workloads, NAS & file, change rates, existing backup metadata associated with the critical materials
- Design and right-sizing – Understanding the data to recommend the best fit model
- Understanding business requirements – What is the data protection strategy; what business challenges should be considered; compliance & regulatory requirements
- Report of recommendations, presentation or quotation

Post contract services and managed service on boarding will be governed by the customer subscribing to the relevant level of service.

Protect	
Backup Assessment	Where an existing Avamar implementation exists, customers can hand management and monitoring of their existing backup to Synapse 360 and realise the benefits of the managed service without redeployment. To ensure that everything can be effectively handed over and supported our engineers will perform a complete assessment of the software versions, configuration, design and backup jobs
Remediation and acceptance	▪ Synapse 360 will make recommendation across the backup and wider infrastructure ▪ Upgrade of software to supported levels ▪ Confirmation that hardware & software is under vendor support ▪ Recommend changes to existing backups and protection levels ▪ Revaluate following remediation actions ▪ Only once all remediation actions are complete the managed service will be on boarded with the Synapse 360 NOC ▪ Implementation of Avamar Virtual Edition for the critical data protection management
Baseline	A baseline will be agreed with an understanding of the data set & timings. This can be used in ongoing troubleshooting, comparison and recommendation.
Agree Process	Synapse 360 has internal change process as defined in our ISO procedures and additionally will incorporate the needs of the customer change control process as much as possible. The customer should nominate contacts who will be trained in the service including how to interact with the NOC, SLA and process.
Design and Deployment	The CRS managed service includes all of the hardware, software and Synapse 360 services required for the effective and efficient backup of the customer's data in addition to the ongoing management and monitoring to recover data from a Cyber Attack. Installation services are included in the cost of the service unless otherwise negotiated on an individual contract basis.
Protection Verification	Customers can decide the protection levels and retention that is right for their business and that is what Synapse 360 will configure.
Testing and Validation	Share with the customer the way that the backups are running, the correct retention levels have been applied, and review any requests for change.

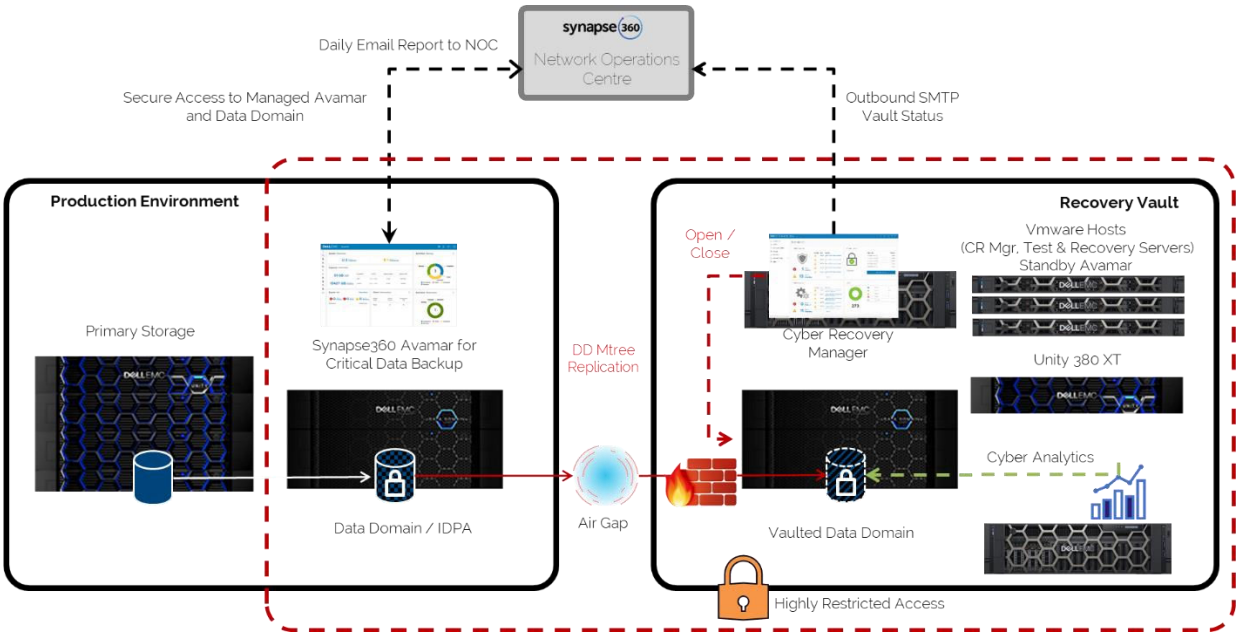
2.3 Service Platform Components

The CRS service will evolve over time and Synapse 360 reserves the right to umbrella (include) additional backup technology from any vendor and twilight (retire) others. Currently the following backup technology can be included in either level of managed service:

- IDPA
- Avamar
- Networker
- Data Domain (Physical only)
- SonicWall
- Dell PowerEdge and PowerSwitch
- Dell Unity

Customers with other backup technologies that they wish to retain wholly or in part within their recovery strategy should contact Synapse 360 for the most up to date compatibility list.

No version information is included in this document but Synapse 360 reserves the right to run the service on a specific version of software and to perform or insist on an upgrade where it would be detrimental to the service not to do so.



2.4 Cyber Recovery Models

The Cyber Recovery solution is based on six sizes to cover the SME market up to large commercial.

- X Small (4TB) - Provides a 4TB DD3300 along with optional recovery infrastructure and analytics. Small may be upgraded to large model
- Small (8TB) - Provides a 8TB DD3300 along with optional recovery infrastructure and analytics. Small may be upgraded to medium and large models
- Medium (16TB) – Provides a 16TB DD3300 along with optional recovery infrastructure and analytics. Small may be upgraded to large model
- Large (32TB) – Provides a DD3300 along with 2x Recovery Servers and 5TB of disk for recovery testing. The 30TB model cannot be upgraded past its maximum.
- X Large (60TB) – Provides a DD6300 along with 3x Recovery Servers and 10TB of disk for recovery testing. It will be possible to upgrade the 60TB model to a 120TB model
- XX Large (120TB+) – Provides a DD6900 along with 4 x Recovery Servers and 20TB of disk for recovery testing. It is possible to upgrade the 120TB version.

Further details on the components are provided below.

Component	Small	Medium	Large
Data Domain Appliance	DD3300-30TB	DD6300-60TB	DD6900-120TB
Recovery Hosts	2 x PowerEdge R440	3 x PowerEdge R440	4 x PowerEdge R440
Analytics Server	1 x PowerEdge R740XD	1 x PowerEdge R740XD	1 x PowerEdge R740XD
Cyber Recovery Manager Server	1 x PowerEdge R740XD	1 x PowerEdge R740XD	1 x PowerEdge R740XD
Recovery Storage	5TB Dell Unity	10TB Dell Unity	20TB Dell Unity
Vault Network	2 x 12 Ports - 10GbE	2 x 12 Ports - 10GbE	2 x 12 Ports - 10GbE
Firewall	SonicWall 3650	SonicWall 3650	SonicWall 4650
Maximum Protected Storage	30TB	60TB	120TB
Minimum Network Requirement	1GbE (10GbE preferred)	10GbE	10GbE
Local Access (Inside Vault)	KVM and iDRAC	KVM and iDRAC	KVM and iDrac
Rack Space	13U	17U	18U

2.5 Managed Service Level Upgrade

Customers initially joining the CRS managed service using an existing Data Domain appliance may upgrade this as part of the service to the Synapse BaaS product.

This is possible at any time within the guidelines below:

- BaaS has a minimum subscription term of 36 months
- Upgrade can be done at any time and is not restricted to CRS contract renewal
- Upgrading will generate a new BaaS agreement with a minimum subscription of 36 months from the time of upgrade
- A new IDPA or Data Domain will be made available to carry out the service
- The migration to BaaS is subject to an assessment by Synapse 360 and acceptance of the new subscription cost by the customer

- New hardware will be provided as part of the upgrade that may take 4-10 weeks to be installed. During this time the CRS managed service will continue
- The Preparation Services described in section 2.2 will be followed for the new service level

It is not currently possible to downgrade between sizes during the contract minimum term. Upon completion of the minimum term customers can request details of a solution that is compatible with Protect.

2.6 Connectivity

The customer is responsible for connectivity from their data centres to operate the service where there is an off-site target. Supported vault targets of the service are:

- Hosted in customer production data centre (separate locked rack with controlled access)
- Hosted in Synapse 360 data centre
- Hosted in customer secondary data centre (separate locked rack with controlled access)

In all configurations it is a requirement that customer provides sufficient bandwidth from their data centre(s) to operate without hindrance negative effect on performance. Connectivity is encrypted over the Internet using a dedicated links, site-to-site VPN or SD-WAN.

The table below summarises the benefits of each location. Primary datacentre refers to the location of the Primary Data Domain. This is preferred due to the ability to cheaply provision 10GbE (or better) networking for replication.

Option	Speed	Security	Cost	Recovery Times	Time to Deliver
Primary Datacentre	**Fastest** Shorter distance between Production	**High** Air gap closed for longest due to proximity to primary data	**Lowest** No 3rd party comms and hosting costs could be cheaper	**Short** Proximity and network speed. Engineers may need to travel to site	**Fastest** no comms links to provision
Recovery Datacentre	**Fast** Dependent on comms links	**High** Air gap open for longer than primary but customer controls physical access	**Highest** Requires separate 10GbE comms link and hosting (additional £5K per month)	**Short** Proximity and network speed. Engineers may need to travel to site	**Longest** Requires link and hosting provisioning
Synapse Datacentre	**Fast** Dependent on comms links	**High** Air gap open for longer than primary but Synapse control physical access	**Highest** Requires separate 10GbE comms link and hosting (additional £5K per month)	**Shortest** Dependent on network speed. Synapse Engineers quicker to recovery site	**Long** Requires link and hosting provisioning but Synapse partners can help with this

Where any one of the above off-site options has been included in the managed service the responsibilities in the table below apply.

Connectivity Responsibilities	
Customer	▪ Provide and fund bandwidth from the customer's data centre of at the level required to effectively run the service ▪ Increase available bandwidth if service requirements grow ▪ Control access into the datacentre where the vault resides ▪ Patch or upgrade on-site equipment if requested to do so in order to effectively operate the service ▪ All ISP charges, support, SLA, management and contracts
Synapse 360	▪ Run a backup assessment that will include bandwidth requirement estimates

	▪ Recommend appropriate bandwidth from customer's site ▪ Provide firewall capable and compatible of terminating IPSEC VPN ▪ Provide bandwidth into the Synapse 360 DC where the managed service includes hosting ▪ Assist with connectivity & security advice to for connectivity
Remote Management	Connectivity is required for remote management for all levels of managed service subscription. **Management Server** ▪ The customer is responsible for ensuring connectivity via secure VPN to all management server IP addresses via LAN/WAN to the Production Avamar VE and Data Domain systems ▪ The customer is responsible for all perimeter devices including switches, routers and firewalls within the customer site required for Synapse 360 access to Avamar VE and Data Domain. ▪ Sufficient bandwidth shall be provided by the customer to allow effective operation of the service

2.7 Licenses & Vendor Support

The ownership and responsibility for the hardware, software, licensing and vendor provided support is dependent on the service level the customer has subscribed to:

- Protect: The customer must provide all software licenses and maintain them under a valid and current support contract with the vendor. It is the responsibility of the customer to ensure that the licenses are valid and that they remain in compliance with all license agreements at all-time throughout the service.
- Atmosphere: Backup licensing and support is bundled in the service and is the responsibility of Synapse 360. The service includes IDPA and we will license the backup for the data and workloads that are specified in scope for the service.
- Azure: Licenses for Azure as a backup target or replication target will be managed by Synapse 360 as part of the service where it is included. Note that this is optional so Azure licenses are not included by default for all customers.

Software & License Ownership	Protect The licenses to operate and use software & hardware remain the property of the customer during and after termination of the service. Atmosphere The licenses to operate and use software & hardware remain the property of Synapse 360 during and after termination of the service.

2.8 Hardware Ownership

Hardware Ownership	Protect The hardware is supplied by the customer and remains the property of the customer during and after termination of the service. Atmosphere

	The hardware is rented to the customer for the duration of the service and remains the property of Synapse 360 at all times during operation and after termination of the service.

2.9 Service Security

The security of the customer's data is of paramount importance to Synapse 360. At all times in operating the service the customer retains full and unconditional ownership of their data.

Synapse 360 NOC Security	The Synapse 360 NOC has been awarded ISO 20000 standard for IT service management covering the following aspects of security: ▪ Physical swipe-card access ▪ Synapse 360 employees only ▪ Procedures & change process ▪ Qualified & experienced engineers
Anti-virus & Malware	All management access from Synapse 360 NOC personnel is performed via the controlled remote desktops that incorporate enterprise anti-virus and anti-malware protection. External email is secured using a 3rd party gateway. Synapse 360 will ensure the protection tools on the management machines within the NOC are updated regularly.
Encryption	The following are encrypted as part of the service: ▪ VPN for management ▪ Data in transit where replication occurs to the Synapse 360 backup cloud ▪ Data in transit where tiering or backup target is Azure ▪ Data at rest in the Synapse 360 backup cloud ▪ Data at rest in Azure

Synapse 360 has a data protection policy in place and complies with GDPR regulation. The Synapse 360 allocated data owner is our Technical Director who will deal with enquiries or notify in the event of a data breach.

3 Operating the Service

There are two levels of the service as described in section 2.3 that give the customer a choice of owning their own backup system that the Synapse 360 NOC operates, or subscribing to a fully developed service that also includes all hardware & software.

When considering the sections below please be aware of the correct service level. Customers can raise additional tickets with the Synapse 360 NOC not outlined in section 3.1 that will be flagged outside the BaaS service and therefore chargeable in line with the rate card. Work outside the service will be quoted and agreed with the customer in advance.

When considering the sections below please be aware of the correct service level. Customers can raise additional tickets with the Synapse 360 NOC that are not outlined in section 3.1 that will be outside the service and therefore chargeable in line with the rate card.

3.1 Common Operations

Common operations are those service tasks that are shared between Protect and Atmosphere level customers. In order to maintain the required high levels of service to our customers it is important to only consider operations within the appropriate subscription level.

3.1.1 Create Backup Schedule

New backup schedule requests can be created for single workloads or datasets, multiple workloads, or full environments.

Objective	Create and verify as working a new backup schedule
Initiation	Customer should request via the NOC primarily using the email helpdesk@synapse360.com or phone 03334 330 911 Only tickets raised using the above method will be tracked and responded to. Customers should not contact NOC personnel direct to make requests
Customer's Responsibility	The following information should be provided: ▪ Contact Name ▪ Company ▪ What is to be protected ▪ Protection schedule ▪ Retention period ▪ Additional narrative where it would be useful to the NOC
Change Request	The above request to the NOC will be acted upon as a change request when made by recognised personnel.
NOC Responsibility	A qualified member of the NOC will: ▪ Respond within the contracted SLA ▪ Assess the change request ▪ Ensure they have all required information ▪ Request clarification if needed ▪ Make the requested change ▪ Inform the customer ▪ Update the ticket
Response	Response time is 4 working hours 8x5x4 (Mon-Fri 9:00-17:00). Expectation: Actions may take longer and this is not a completion time. The NOC will respond via email
Completion	Once the NOC believe the request to be completed the ticket will be closed.
Tracking	Requests can be tracked via the online portal: https://ww4.autotask.net/ClientPortal/
Escalation	Customers can request escalation by phone 03334 330 911 and asking to speak to the Service Desk Manager.

3.1.2 Amend or Delete Backup Schedule, Amend Retention Settings

Change of content requests can be created for single workloads or datasets, multiple workloads, or full environments. This may also be to change the time or date of a backup schedule, or place a job on hold during a maintenance period.

Objective	Amend and verify as working an existing backup schedule
Initiation	Customer should request via the NOC primarily using the email helpdesk@synapse360.com or phone 03334 330 911

	Only tickets raised using the above method will be tracked and responded to. Customers should not contact NOC personnel direct to make requests
Customer's Responsibility	The following information should be provided: ▪ Contact Name ▪ Company ▪ Clearly identify without ambiguity the job that is to be amended ▪ Changes that are to be made ▪ Additional narrative where it would be useful to the NOC
Change Request	The above request to the NOC will be acted upon as a change request when made by recognised personnel.
NOC Responsibility	A qualified member of the NOC will: ▪ Respond within the contracted SLA ▪ Assess the change request ▪ Ensure they have all required information ▪ Request clarification if needed ▪ Make the requested change ▪ Inform the customer ▪ Update the ticket
Response	Response time is 4 working hours 8x5x4 (Mon-Fri 9:00-17:00). Expectation: Actions may take longer and this is not a completion time. The NOC will respond via email
Completion	Once the NOC believe the request to be completed the ticket will be closed.
Tracking	Requests can be tracked via the online portal: https://ww4.autotask.net/ClientPortal/
Escalation	Customers can request escalation by phone 03334 330 911 and asking to speak to the Service Desk Manager.

3.1.3 Schedule a Restore

A restore of a dataset, file or virtual machine can be requested to the same location (overwrite) or alternative location. If not specified, the restore will be made from the latest valid backup of that dataset.

Objective	Successful restore of a file, dataset or virtual machine
Initiation	Customer should request via the NOC primarily using the email helpdesk@synapse360.com or phone 03334 330 911 Only tickets raised using the above method will be tracked and responded to. Customers should not contact NOC personnel direct to make requests

Customer's Responsibility	The following information should be provided:
	▪ Contact Name
	▪ Company
	▪ Clearly identify without ambiguity the data that should be restored
	▪ Identify the date that the restore should be made to
	▪ The location of the restore
	  ○ Same location (overwrite) existing data will be lost
	  ○ Alternate location (redirect) specify location
	▪ Additional narrative where it would be useful to the NOC

Change Request	The above request to the NOC will be acted upon as a change request when made by recognised personnel.

NOC Responsibility	A qualified member of the NOC will: ▪ Respond within the contracted SLA ▪ Assess the change request ▪ Ensure they have all required information ▪ Request clarification if needed ▪ Make the requested change ▪ Inform the customer ▪ Update the ticket
Response	Response time is 4 working hours 8x5x4 (Mon-Fri 9:00-17:00). Expectation: Actions may take longer and this is not a completion time. The NOC will respond via email
Completion	Once the NOC believe the request to be completed the ticket will be closed.
Tracking	Requests can be tracked via the online portal: https://ww4.autotask.net/ClientPortal/
Escalation	Customers can request escalation by phone 03334 330 911 and asking to speak to the Service Desk Manager.

3.1.4 Test Restore

The customer may from time to time wish to request test restores to validate backups and ensure their retention is valid. This may be for audit reasons or simply peace of mind.

Objective	Test restoration of each data type from a specific backup set
Initiation	Customer should request via the NOC primarily using the email helpdesk@synapse360.com or phone 03334 330 911 Only tickets raised using the above method will be tracked and responded to. Customers should not contact NOC personnel direct to make requests
Customer's Responsibility	The following information should be provided: ▪ Contact Name ▪ Company ▪ Identify the backup date to be restored ▪ Identify any specific data that should be included in the test ▪ Additional narrative where it would be useful to the NOC
NOC Responsibility	The above request to the NOC will be acted upon as a change request when made by recognised personnel. Upon verification that the backup set was valid the NOC will: ▪ Always perform test restores to an **alternate location** ▪ Validate each data type has restored successfully **without risk** to live systems or data ▪ Provide confirmation via email that the test was / was not successful ▪ Clean up and delete any temporarily restored data or virtual machines
Response	A qualified member of the NOC will: ▪ Respond within the contracted SLA ▪ Assess the change request ▪ Ensure they have all required information ▪ Request clarification if needed ▪ Make the requested change ▪ Inform the customer

	▪ Update the ticket
Completion	Response time is NBD working hours 8x5x4 (Mon-Fri 9:00-17:00). Expectation: Actions may take longer and this is not a completion time. The NOC will respond via email
Escalation	Once the NOC believe the request to be completed the ticket will be closed.
	Requests can be tracked via the online portal: https://ww4.autotask.net/ClientPortal/
	Customers can request escalation by phone 03334 330 911 and asking to speak to the Service Desk Manager.

3.1.5 Emergency Restore

Change of content requests can be created for single workloads or datasets, multiple workloads, or full environments. This may also be to change the time or date of a backup schedule or place a job on hold during a maintenance period.

Objective	Successful restore of a file, dataset or virtual machine
Initiation	Customer should request via the NOC primarily using the email helpdesk@synapse360.com or phone 03334 330 911 **The Service Desk Manager reserves the right to assess the urgency of an Emergency Restore request for reasons of prioritisation.** Only tickets raised using the above method will be tracked and responded to. Customers should not contact NOC personnel direct to make requests

Customer's Responsibility	The following information should be provided:
	▪ Contact Name
	▪ Company
	▪ Clearly identify without ambiguity the data that should be restored
	▪ Identify the date that the restore should be made to
	▪ The location of the restore
	  o Same location (overwrite) existing data will be lost
	  o Alternate location (redirect) specify location
	▪ Additional narrative where it would be useful to the NOC

NOC Responsibility	The above request to the NOC will be acted upon as a change request when made by recognised personnel.
Response	A qualified member of the NOC will: ▪ Respond within the contracted SLA ▪ Assess the change request ▪ Ensure they have all required information ▪ Request clarification if needed ▪ Make the requested change ▪ Inform the customer ▪ Update the ticket
Completion	Response time is 2 working hours 8x5 (Mon-Fri 9:00-17:00). Expectation: Actions may take longer, and this is not a completion time. The NOC will respond via email
Escalation	Once the NOC believe the request to be completed the ticket will be closed.

	Customers can request escalation by phone 03334 330 911 and asking to speak to the Service Desk Manager.
Ticket Tracking	Requests can be tracked via the online portal: https://ww4.autotask.net/ClientPortal/

3.2 Software Upgrades & Hardware Patching

See also '2.7 License & Vendor Support' and '2.8 Hardware Ownership'.

Service Level	Responsibility
Protect	▪ The customer is responsible for providing the licenses and access to software or firmware downloads ▪ The customer will provide a means to download the updates or copy them to the required location or management server ▪ Synapse 360 will, at our discretion where it is beneficial to the running of the service, upgrade major software versions as they become available ▪ Minor software updates, releases and bug fixes will not be installed unless Synapse 360 deems it necessary to the running of the service ▪ Hardware patches will not be installed unless Synapse 360 deems it necessary to the running of the service
Atmosphere	▪ Synapse 360 is responsible for providing the licenses and access to software or firmware downloads ▪ The customer will provide a means to download the updates or copy them to the required location or management server ▪ Synapse 360 will, at our discretion where it is beneficial to the running of the service, upgrade major software versions as they become available ▪ Minor software updates, releases and bug fixes will not be installed unless Synapse 360 deems it necessary to the running of the service ▪ Hardware patches will not be installed unless Synapse 360 deems it necessary to the running of the service
Working Hours	Synapse 360 will perform upgrades or patches in accordance with the above during working hours only 8x5. The customer may request for work to be carried out at other times which will be agreed in advance and will be chargeable in accordance with the Synapse 360 rate card.

4 Supporting Services

4.1 Service Monitoring & Alerting

Customers may raise tickets as described in this document and daily checks will be performed by the Synapse 360 NOC in carrying out the service. In addition, automatic alerting will be configured as shown in the table below.

Protect	▪ The level and detail of monitoring is governed by the hardware and software supported. See '2.1 Supported Products' ▪ The capability of the software may restrict the type and detail of the alerting ▪ Alerting will be configured to the Synapse 360 NOC support mailbox

	▪ The customer will facilitate the sending of alerts to the Synapse 360 NOC using SMTP relay with their mail server or provider ▪ The customer is responsible for ensuring the continued support for sending SMTP alerts
Atmosphere	▪ Alerting will be configured to the Synapse 360 NOC support mailbox ▪ The customer will facilitate the sending of alerts to the Synapse 360 NOC using SMTP relay with their mail server or provider ▪ The customer is responsible for ensuring the continued support for sending SMTP alerts
Monitored Alerts	▪ Backup or Restore Job incomplete ▪ Backup or Restore Job failure ▪ Hardware or Software Failure
Severity	▪ All Critical level events ▪ No warning level events ▪ No informational alerts will be monitored Alerts generated by BaaS are non-service affecting and therefore not considered to be Sev1 or Sev2 at any time.
Response	Response time is 4 working hours 8x5x4 (Mon-Fri 9:00-17:00)

4.2 Service Reviews

Service reviews are remote meetings held between the customer and the Service Delivery Manager or Service Owner. These are to be held quarterly to discuss the performance of the service, its effectiveness and to identify any future expansion.

Frequency	Quarterly. The frequency of the meeting can be varied by request
Attendees	Synapse 360: Service Delivery Manager or Service Owner Customer: Subscription Owner or IT Manager
Format	Remote via Google meeting / Webex / teleconference or similar
Deliverable	Meeting only
Content Summary	Standardised presentation showing some or all of the following. The content of the report or discussion is subject to change: ▪ The effectiveness of the service ▪ Service against SLA ▪ Growth and future expansion ▪ Changes to the service (requested or suggested) ▪ Options that may be applicable (cloud tier, replication) ▪ Recurring issues ▪ Recommended infrastructure actions ▪ Requests for change
Other Meetings	Additional meetings can be arranged by request including those with 3rd parties and introduction to other Synapse 360 products or services

5 Service Charges

Synapse 360's policy for billing BaaS is monthly in advance from the agreed date that the service is live. There is generally no additional charge for setting up the service except where agreed remediation is required to bring a system to the required supportable level (Protect).

Additional Synapse 360 Professional Services that are identified will be performed outside the service. For example, this may be infrastructure changes required to support BaaS, installation of agents or networking.

Contract Term	Protect: 12-36 Months Atmosphere: 36-60 Months
Minimum Term	Protect: 12 Months Atmosphere: 36 Months
Invoice Frequency	Invoicing is monthly in advance
Charging Basis	Charge for the service is calculated on the following: ▪ Amount of data (raw) GB/TB ▪ Service level (Protect or Atmosphere) ▪ Number of virtual machines to be protected ▪ IDPA model specified (Atmosphere) ▪ Cloud capacity (Synapse 360 Backup Cloud) ▪ Cloud capacity & license agreement (Azure) ▪ Number of backup servers & targets
Scaling Basis	The service scales on a monthly basis using the metrics above (charging basis). There may be a lead time where new hardware is required or if a customer transitions from Protect to Atmosphere level service.

6. Service Exclusions or Limitations

Synapse 360's Backup as a Service (BaaS) gives customers the confidence that they can protect and recover essential current and historic data without the need to maintain skills or provide staff resources in-house. Additionally, Synapse 360 will manage the associated licenses and hardware support, maintain the software to a version recommended by us, and deal with any support incidents relating to backups.

Other complimentary services are available but are not included in BaaS. The table below addresses some common exclusions from the BaaS services. The list is not exhaustive; only products or services expressly outlined in this document as being in scope

Exclusions	1. Synapse 360 does not own the data, access, permissions 2. Synapse 360 is not responsible for any loss of data, deletion, overwrite, amendment or inability to find or restore data from backup or archive. This relates to content that may no longer be present within the source backup (Cyber or replication DD) or source location (server, SAN), and therefore no longer present in the backup or cyber replication to be recovered from the final device. 3. Physical or virtual network or firewall configuration or design 4. Consultancy on infrastructure, storage, virtual environment, NAS, SAN or any live systems 5. Consultancy around software, permissions, upgrades, version, configuration, modification, programming 6. Deployment of physical or virtual machines 7. Operating systems, software or configuration of any virtual or physical machine to be protected by the service 8. Configuration of the firewall for VPN termination on the customer's site, responsibility for compatibility 9. Performance of any Internet, WAN or cloud connect link used for, or affecting the performance of, the service 10. Upgrade of any infrastructure element including but not limited to virtual infrastructures, hypervisor, operating systems, applications, drivers, hardware driver or bios. 11. Any full system recovery, disaster recovery from backup 12. Out of hours work planned or unplanned 13. Monitoring of any system or metric outside the core backup managed service as described in this document 14. Monitoring of networks, connectivity, security 15. Security policy for remote access, remote management or remote monitoring within the Customer network 16. Creation of users, permissions or policies to allow remote management and monitoring of the service 17. Configuration of mail servers or external mail services to support the required SMTP alerting 18. Patching of any infrastructure component

7 Service Levels (SLA)

7.1 SLA Definitions

This section relates to the Foresight Business Critical (Foresight Support) service levels only. The Synapse 360 Foresight Support managed service is covered by three levels of service level to provide our customers with complete confidence:

- Contractual service level agreement (C-SLA) – As defined in the customer contract this outlines the metrics of service performance and how it is measured. Synapse 360 commits to delivering the contracted service to the agreed levels and outlines any penalties or credits resulting from failure to meet these standards.
- Response time service level agreements (RT-SLA) – As laid out in the service definition the response that our customers can expect for a contracted service in the event of a customer initiated action or automated event.
- A managed service level SLA (MS-SLA) – Our commitment to the level of service interaction between Synapse 360 and the customer in carrying out the managed service.

7.2 SLA Remediation

SLA Category	Remediation	Action
C-SLA	Contract enquiries will be escalated to a Synapse 360 director to consolidate the points raised against the service design and contractual wording	Determined by the director responsible for the service this may include amendment to the service or internal training to ensure the proper operation of the service
RT-SLA	Response enquiries will be escalated to the Service Delivery Manager to investigate the circumstances in which timescales were missed	Root cause analysis (RCA) will be presented to the customer. Internal training may be result or amendment to ISO procedure within the NOC
MS-SLA	Managed Services are measured against customer satisfaction levels and verified by surveys carried out for Synapse 360 by an external company	Customer satisfaction in our managed services and by extension our people is a board backed priority across the business

Where any of the above are found to be lacking or below the required standard the Service Delivery Manager (SDM) will request a remediation schedule with the customer. The result is more frequent meetings with a senior member of the Synapse 360 management team (the SDM). The schedule suggested will be weekly – monthly whilst remediation actions are agreed and carried out.

We invite customers to choose the remediation schedule that best suits them and work together to a successful outcome.

Where the SLA is not met at the start of a contract term the Synapse 360 SDM may elect to defer the payment start date for that service until such a time that it can be fully and satisfactorily implemented.

8 Service Term Maturity

Upon completion of the contract term, where it has not been extended, Synapse 360 will continue to provide DaaS and invoice the customer on a monthly basis. During this rolling period the customer will continue to enjoy the full features of the storage and Foresight support for as long as they continue to settle the invoice amount.

The customer has a number of choices at service term maturity:

DaaS Service Continuance (Do nothing)	In the event that the customer elects to 'do nothing' at service maturity: ▪ The customer will continue to be invoiced the same monthly subscription ▪ Invoice Frequency: Monthly in advance ▪ DaaS Hardware & software will continue to be available for customer use for as long as they continue to settle the invoiced amount ▪ Synapse 360 Foresight configuration, monitoring and troubleshooting will continue 5x5 & 24x7 for P1 & P2 ▪ Some vendor hardware or software support may become unavailable where: o It is not available to Synapse 360 on a monthly subscription i.e. annualised support will not be purchased during a service continuance o Any product, license or component has reached end of service life (eosl) ▪ Limitations in service or escalated risk may result where back to back vendor support is not in place. This risk rests exclusively with the customer
DaaS Contract Renewal	This is the usual outcome. Working with the account executive the customer chooses to renew the contract in one of two modes: 1. Where the DaaS comprises technology that is not eosl and is deemed fit for the business, the customer may renegotiate in increments of (min) 12 months. a. In this scenario the service will be supported by back-to-back vendor support and can be upgraded on demand b. The service will essentially continue for 12 months as defined in the service definition c. The commercial agreement may be revisited with the account executive every 12 months 2. The customer can choose to enter into a new DaaS or PDCS agreement for a minimum of 36 months a. Synapse 360 will reassess the environment and propose a new DaaS managed service as laid out in this document

	b. New hardware and software will be implemented to support the renewed DaaS c. Migration planning & testing will commence
Termination of DaaS	The customer may choose to terminate part or all of the DaaS service at the end of the full term. Synapse 360 will, at best endeavours, assist the customer in the planning and enable migration of storage away from the DaaS. ▪ Where notice of termination is given by the customer Synapse 360 will continue to manage the storage and provide the full service use for as long as the customer continues to settle the invoiced amount ▪ The customer will continue to be invoiced the same monthly subscription until all data is removed and 100% of Synapse 360 owned hardware and software is recovered (3rd party data centre is utilised for the service) ▪ Invoice Frequency: Monthly in advance ▪ All hardware & software remains the property of Synapse 360 ▪ Synapse 360 will, on a best endeavours basis, assist with the removal of customer data
Option to Buy	Synapse 360 will, upon successful negotiation, sell the components of the DaaS to the customer and transfer ownership.