



Managed Service Definition

PowerCloud Protect

Version 1.4

Contents

1 PowerCloud Protect Introduction	4
2 Service Scope	5
2.1 Service Packages	5
2.2 Preparation Services	8
2.3 Day 2 Operations Feature Comparison.....	10
2.4 Service Platform Components	11
2.5 Service Level Upgrade	12
2.6 Connectivity.....	12
2.7 Licenses & Vendor Support	13
2.8 Hardware Ownership.....	14
2.9 Service Security	14
3. Operating the Service	14
3.1 Operating Synapse 360 PowerCloud Managed Service	14
3.2 Requesting Upgrades or Service Extensions	14
4 Supporting Services.....	15
4.1 Service Monitoring & Alerting	15
4.2 Service Reviews	15
5 Service Charges	15
6 Service Exclusions or Limitations	16
7 Service Levels (SLA) PowerCloud Protect Operations	17
7.1 SLA Definitions	17
7.2 SLA Remediation.....	17
8 Service Term Maturity	17

Document Purpose

The intended audiences for this document are below.

Internal Synapse360 employees.

- To ensure consistency of expectations between sales, presales and manage service operators who execute customer tasks from the Managed Service Centre (MSC).
- To provide the basis for the MSC and contracts team to scope and provide the best quality managed service to the customer.
- To enable the Service Delivery Manager (SDM) to evolve the managed service to continuously improve the customer experience.

External Customers & Partners

- 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:	General Release
Issue Version:	1.4
Date of Issue:	31/03/2023

Amendment Summary

Issue	Date	Commentary	Initials
0.1	28/02/2019	Initial draft document	SD
1.0	01/06/2019	Document release & Service Manager Acceptance	SD
1.1	11/02/2020	Amendment: 'Service Term Maturity'	SD
1.2	02/02/2021	Branding	SD
1.3	01/09/2022	Updated product portfolio	SD
1.4	30/06/2023	Updated PowerCloud branded and operational feature matrix	JP

1 PowerCloud Protect Introduction

PowerCloud Protect offers effortless data protection and recovery, eliminating the need for in-house resources. We manage licenses, hardware support, software maintenance, and handle any data recovery incidents. Our experts will monitor backups, provide periodic reports, perform software updates, and conduct restores for you.

PowerCloud Protect is available with several versions:

Operational Services

- **PowerCloud Protect Operations:** Provides a team of architects, engineers, administrators, and customer success managers to ensure that customers are informed and making the best use of their technology. The Managed Service operation services that ensure customers data is continuously protected and recoverable. May be used in conjunction with any of the PowerCloud services below or any customer owned or rented investments.

Technology Services

- **PowerCloud Protect Backup:** A turnkey solution which includes the hardware, software that ensures data is protected and recoverable. PowerCloud Protect Operations is a recommended add-on.
- **PowerCloud Protect Cyber Vault:** An option for customers requiring an immutable air-gap backup as part of an approach to cyber-risk mitigation. Includes all hardware, software costs, maintenance, and managed service operators (PowerCloud Protect Operations).
- **PowerCloud Disaster Recovery:** Provides a secondary platform, replication technology, maintenance services and managed service operators (PowerCloud Protect Operations) for fast recovery and continuous remote protection.

Key Facts

- 8x5 backup management from the Synapse 360 Network Operation Centre (MSC)
 - 24x7x365 response for critical failures and recovery support
 - Includes unlimited restores.
 - OPEX model includes hardware & software licensing.
 - ISO 20000 and ISO 27001 accredited Synapse 360 MSC / Datacentres
 - All data is encrypted in transit and at rest.
 - Choose where your data resides: on-premises, in a Synapse 360 UK or IOM based data centre, or in the public cloud with Microsoft Azure
-
- Major software version upgrades are included where they are available via a valid license agreement and recommended by the Synapse360 PowerCloud Protect teams.
-
- Optional Cyber Vault provides an automated retention locked and air gapped copy of a backup data to mitigate against cyber attack

Vendor Terms

All hardware and software that is involved in the service must be under a current vendor support agreement. The service level from Synapse360 will immediately default to 'best endeavours' where vendor support has expired.

Ordering Information

PowerCloud Protect is a comprehensive solution that includes everything needed for successful data recovery. The service supports technologies from Dell Technologies, Veeam, Microsoft and Veritas. Other backup technologies may be added in future.

There are two options available depending on whether the customer already owns hardware and software compatible with the managed service:

1. PowerCloud Protect Managed Service – For customers who wish to continue using their current backup software or wish to transition at a later date.
2. PowerCloud Protect single subscription including base management, monitoring, hardware & software. Recommend combining with PowerCloud Managed Service to ensure full data protection and recovery outsourcing to Synapse360. This may include one or all of the following capabilities:
 - PowerCloud Protect Backup
 - PowerCloud Protect Cyber Recovery
 - PowerCloud Protect Disaster Recovery

2 Service Scope

This section details the scope of the service.

- **Service Package:** Defines the service capabilities.
- **Preparation Services:** Activities that will be carried out during acceptance or on-boarding.
- **Day 2 Operations Feature Matrix:** The included service features included with each product in the PowerCloud Protect suite.
- **Service Platform Components:** The software, hardware and Cloud components provided within the service.

Services outside of scope will require prior agreement and will be charged for at our standard rate.

2.1 Service Packages

Key Service Package Information	
Objective	▪ To ensure recoverability of customer data in the event of data loss, disaster, or cyber-attack. ▪ Remove the operation dependency and cost associated with in house management of data protection and recovery
Supported From	▪ The secure ISO 20000 accredited Synapse 360 Managed Services Centre (MSC). ▪ UK and Isle of Man based MSCs ▪ No work is ever outsourced. ▪ Vendor escalation is 100% supervised by the MSC
Access and Security	▪ Secure access to the backup and recovery systems from our MSC ▪ Connection will be via encrypted site-to-site VPN. ▪ Access to customer stakeholders for restore instruction

Support Levels	
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. ▪ Noncritical: 9AM to 5PM, Monday to Friday ▪ Critical 24x7x365: (subject to Premium Service uplift) Response 1 hour ▪ Support Response for in-scope data protection infrastructure ▪ Outside of in-scope infrastructure is not subject to support levels and will incur additional cost

Engagement Scope	
Tasks Outline	▪ Monitor and manage data protection scheduled jobs (backup, replication, integrity) ▪ Receive change requests from the customer to amend, create or delete protection jobs ▪ Receive change requests from the customer to perform test, overwrite or alternative location restores ▪ Customers may raise ticket requests via email or phone and monitor directly using the Synapse360/MT Group customer portal ▪ Provide quarterly updates with backup success rates, high level data insight, data growth, recurrent issues, recommendations

Supported Products PowerCloud Protect Backup	PowerCloud Protect Backup supports the following products: Hardware \ Virtual Appliances: ▪ Dell Integrated Data Protection Appliance (IDPA) ▪ Dell Data Domain (Virtual or Physical) ▪ Dell ECS ▪ Dell PowerProtect Data Manager (PPDM) ▪ Dell PowerVault Software: ▪ AvePoint Cloud Backup ▪ Dell APEX Backup Services ▪ Dell Avamar ▪ Dell Data Protection Suite (DPS) for Backup ▪ Dell DDBoost ▪ Dell Networker ▪ Dell PowerProtect Snapshot Manager ▪ Druva Cloud Backup ▪ Microsoft Azure Backup ▪ Microsoft Azure Site Recovery ▪ RecoverPoint Classic ▪ RecoverPoint for Virtual Machines ▪ Veeam Backup & Replication ▪ Veritas Backup Exec Recovery Locations: ▪ Customer owned or leased datacenter ▪ Synapse360 datacenter partner or Isle of Man datacenter ▪ Microsoft Azure
Supported Applications & Operating Systems	For a list of supported Hypervisors, Operating Systems and Applications please consult the PowerCloud Protect Support Matrix
Supported Products PowerCloud Protect Cyber Vault	Specific products related to the PowerCloud Protect Cyber Vault. None Dell solutions may limit the effectiveness of the Cyber Vaults ability to detect compromises in the vault. Hardware: ▪ Dell Data Domain ▪ Dell PowerEdge ▪ Dell SonicWALL Firewall ▪ Dell PowerConnect ▪ Dell PowerStore Software: ▪ Dell Avamar ▪ Dell Cyber Recovery Manager ▪ Dell Data Protection Suite (DPS) for Backup ▪ Dell DDBoost ▪ Dell Networker ▪ Index Engines CyberSense ▪ Microsoft Hyper-V \ Azure Stack HCI ▪ Veeam Backup & Replication ▪ Veritas Backup Exec ▪ VMware vSphere Recovery Locations: ▪ The location of the Cyber Vault only this may be: ▪ Customer owned or leased datacenter. ▪ Synapse360 datacenter partner or Isle of Man datacenter

Supported Products PowerCloud Protect Disaster Recovery	The Disaster Recovery option managed service includes the following products. Software: - RecoverPoint Classic and RecoverPoint for Virtual Machines - Veeam Backup & Replication - Vmware Replication - Microsoft Azure Site Recovery Recovery Locations: - Customer owned or leased datacenter. - Synapse360 datacenter partner or Isle of Man datacenter - Microsoft Azure
PowerCloud Protect Operations Boundary ⁽¹⁾	PowerCloud Protect Backup operational services cover all aspects of the supported backup and recovery infrastructure. The customer is responsible for: - Core data infrastructure (Production data) - Data integrity - Virtual machines, operating systems, applications, and agents (including but not limited to xVSS, VMware Agent). PowerCloud Protect Cyber Vault operational service starts with vault replication and ensures an air gapped data protection and recoverability. Where the customer has not subscribed to PowerCloud Backup service they are responsible for all aspects of backup, such as: - Infrastructure - Software - Operation (including but not limited to creating and managing backup jobs, restoration of data, troubleshooting and remediating backups). PowerCloud Protect Disaster Recovery covers the replication and continuous protection engine, Consistency Groups and associated policies. It is the customer's responsibility to submit a change request for any alterations to the recovery systems.
Infrastructure Requirements	Delivery of the PowerCloud Protect services will require the customer to provide some or all of the following: - Data Centre facility and connectivity for the backup appliances - Compute and Protect resources for backup and management systems where required. - Secure Internet connection for management access Synapse360 Teams will provide details of these requirements during the onboarding stage.
Review and Update	- Customers will mainly interact with the Synapse 360 MSC. - Quarterly remote Teams updates are provided to review the service and discuss any recommendations or remediation. - Technical Account Management may be aligned to multi-product subscribers to ensure the on-going value and integration across all services
Out of Scope	- Disaster recovery, full system restores (unless PowerCloud Protect Disaster Recovery option is chosen) - Out of hours emergency restores or work that continues beyond the 8x5 service hours unless Premium Managed Service (24x7x365 option is taken).

⁽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 MSC 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 MSC creates a manual protection task to run at another time.

2.2 Preparation Services

The following tasks will be undertaken by Synapse360 are provided free of charge (FOC) prior to contract:

- Assessment and sizing – Using our toolsets to assess current Protect requirements, performance, IOPS, requirements, and business needs and desires, baseline and what 'good' looks like
- Design and right-sizing – Understanding access types, performance, growth and technology suitability.
- Understanding business requirements – Scale & performance; security policy; what business challenges should be considered; compliance & regulatory requirements.
- Report of recommendations, presentation, or quotation

Post contract services and managed services on boarding will be governed by the 'Business Critical' level of service as defined in the managed service definition 'MSD-PowerCloud-Support-xx.docx'.

PowerCloud Protect Backup	
Design and Deployment	Consultancy and implementation services are included in the cost of the service unless otherwise negotiated on an individual contract basis.
Protection Verification	Under consultation with Synapse360 experts the customer will decide the protection levels and retention that is right for their business.
Testing and Validation	Share with the customer the way that the backups are running, the correct retention levels have been applied, data can be restored and review any requests for change.
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 an 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 and who will be trained in the service including how to interact with the MSC, SLA and process.

PowerCloud Protect Cyber Vault	
Design and Deployment	Installation services are included in the cost of the service unless otherwise negotiated on an individual contract basis.
Protection Verification	Air Gap data that enters the vault is also retention locked using the built-in governance functionality. The Vault Manager is responsible for reporting on the replication and protection of data to the Synapse 360 MSC.
Testing and Validation	Share with the customer the replication is working properly, correct retention levels have been applied, data can be recovered and review any requests for change.
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 an 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 and who will be trained in the service including how to interact with the MSC, SLA and process.

PowerCloud Protect Disaster Recovery	
Protection Assessment	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 the VMs that require protection.
Remediation and acceptance	Synapse 360 will make recommendations across the recovery and wider infrastructure to achieve the desired RTO and RPO. This may include: ▪ Upgrade of software to supported levels. ▪ Confirmation that hardware & software is under vendor support. ▪ Recommend changes to existing workloads and application including P2V operations as required. ▪ Reevaluate following remediation actions. Only once all remediation actions are complete the managed service will be on boarded with the Synapse 360 MSC
Design and Deployment	Installation services are included in the cost of the service unless otherwise negotiated on an individual contract basis.
Protection Verification	Air Gap data that enters the vault is also retention locked using the built-in governance functionality. The Vault Manager is responsible for reporting on the replication and protection of data to the Synapse 360 MSC.
Testing and Validation	Share with the customer the replication is working properly, correct retention levels have been applied, data can be recovered and review any requests for change.
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 an 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 and who will be trained in the service including how to interact with the MSC, SLA and process.

Backup Managed Service (Customer Owned Technology)	
Backup Assessment	To accurately scope Synapse360 will undertake an assessment of: ▪ Data types and volumes ▪ Software versions ▪ Hardware configurations ▪ RTO\RPO ▪ Retention requirements ▪ Application, OS, and hypervisors
Remediation and acceptance	The following may be required to prepare the customer environment: ▪ Upgrade of software to supported levels. ▪ Confirmation that hardware & software is under vendor support. ▪ Recommend changes to existing backups and protection levels. ▪ Reevaluate the solution following remediation actions. Only once all remediation actions are complete the managed service will be on boarded with the Synapse 360 MSC
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	Synapse360's change process is defined in our ISO procedures and will incorporate the needs of the customer change control process as much as possible. The customer will nominate up to 5 contacts who will be trained in the service including how to interact with the MSC, SLA and process.

2.3Day 2 Operations Feature Comparison

PowerCloud Protect provides operational processes, monitoring and troubleshooting of the customer's protection and recovery environment. This service is not intended to take the place of business continuity planning or associated services. Out of hours restoration, and rebuilding of the customer's working environment from a backup is out of scope.

The table below outlines the features for each PowerCloud Protect product. These features are Day 2 operations (post onboarding and go live)

☑ Full functionality,  Not Supported \ Chargeable - N/A ▲ Partially Supported \ Missing full capability

Feature	n	PowerCloud Protect Backup	PowerCloud Protect Disaster Recovery	PowerCloud Protect Cyber Vault
License Management	☑	☑	☑	☑
Software Licenses Included		☑	☑	☑
Critical Release Software Updates	☑	☑	☑	☑
Hardware upgrade maintenance ⁽²⁾	☑	☑	☑	☑
Agent Deployment & Configuration	☑			
Primary Backup Hardware \ Virtual Appliance Included ⁽²⁾		☑	-	
Primary Backup Software Included ⁽²⁾		☑	-	
Disaster Recovery Platform Included ⁽²⁾		-	☑	-
Disaster Recovery Replication & Orchestration Software Included ⁽²⁾		-	☑	-
Cyber Recovery Vault Hardware Included ⁽²⁾			-	☑
Cyber Recovery Software Included ⁽²⁾			-	☑
Recovery Location Provided		-	☑	On request
In Contract Capacity Upgrades	☑	☑	☑	☑
Customer Monitoring Access	☑	☑	☑	☑
Growth Trends & Data Analysis	☑	☑	☑	☑
PowerCloud Protect Platform Support	☑	☑	☑	☑
1 Hour Critical Response SLA (Platform Down)	☑	☑	☑	☑
3rd Party escalations	▲	☑	☑	☑
Quarterly Report	☑	☑	☑	☑
Quarterly Performance Review & Advisory	☑			
Unlimited Access to Qualified and Experienced Experts	☑			
Access to Synapse360 Support Personnel	☑	☑	☑	☑
Troubleshooting & RCA	▲	☑	▲	☑
Protection Job Creation	☑			
Protection Job Modify	☑			
Protection Job Delete	☑			
Protection Job Restore	☑			
Protection Job Failure Monitoring	☑			
Monthly Random or Customer Chosen Data Recovery Test Restore (100GB Max)	☑			
Protection Job Remediation & Recommendation	☑			
Replication Job Configuration	☑			
Troubleshooting & RCA	☑			

Protection or Recovery Related Network configurations	✓			
Hardware optimization	✓			
Security hardening, scanning	✓			
Policy changes	✓			
Restore testing	✓			
Replication testing, Optimizing, configuring	✓			
Cyber Vault Critical material analysis, review, and maintenance	✓	-	-	
Customer runbook maintenance, creation, optimization, communication	✓			
Recovery Firewall configurations	✓			
Recovery Switch configurations	✓			
Twice Yearly Recovery Drills (select data up to 10 workloads, 1TB data)	✓			
8x5x4 Hour Response from Synapse 360 ISO Accredited MSC	✓	✓	✓	✓
8x5x1 Hour Response from Synapse 360 ISO Accredited MSC for Urgent Data Restore ⁽³⁾	✓			
Raise tickets via Phone, Email, Online Portal	✓	✓	✓	✓
On-going consultancy and technical account management	✓	✓	✓	✓
Support hour allowance per month	50 per service	10	10	10

- ⁽²⁾ Subject to the approved design and purchased subscription. Hardware & software provided within the managed service subscription cost remains the property of Synapse 360 at all times and is rented to the customer for their sole use for the term of the contract. The customer is responsible for ensuring the hardware if it is installed outside a Synapse 360 data centre.
- ⁽³⁾ Customers may, from time-to-time request business critical file or data restores. Once this has been accepted by the Synapse 360 MSC as business critical, they will endeavour to provide an accelerated response. Additionally customers may uplift their service to Premium for 24x7x365 support.

2.4 Service Platform Components

Synapse 360 reserves the right to umbrella (include) additional protection and recovery technology from any vendor and twilight (retire) others. Currently the following data protection technology specified in **Section 2.1** is supported.

Customers with additional data protection technologies that form part of their protection strategy should contact Synapse360 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.

The Synapse360 Sales Account Manager and Technical Architects will establish the best fit combination of supported configurations for the customer.

2.5 Service Level Upgrade

Customers initially subscribing to the PowerCloud Protect Operations on their own technology may wish to extend the term of the contract and migrate to PowerCloud Protect Backup, Disaster Recovery or Cyber Vault when their own protection software licenses expire, or when protection hardware becomes end of life.

This is possible at any time within the guidelines below:

- PowerCloud Protect has a minimum subscription term of 36 months.
- Upgrade from PowerCloud Protect Operations to PowerCloud Protect Backup, Disaster Recovery or Cyber Vault can be done at any time and is not restricted to contract renewal.
- Moving from PowerCloud Protect Operations to any other PowerCloud Protect service will generate a new agreement with a minimum subscription of 36 months from the time of upgrade.
- New hardware and software will be provided as part of the contract.
- It is not possible to adopt any customer backup hardware or software as part of the PowerCloud Protect range.
- The migration from PowerCloud Operations to any other PowerCloud Protect service is subject to an assessment by Synapse360 and acceptance of the new subscription cost by the customer.
- New hardware will be provided as part of the upgrade that may take 8-10 weeks to be installed. During this time the PowerCloud Protect Managed service will continue
- The Preparation Services described in section 2.2 will be followed for the new service level.
- Addition of PowerCloud Cyber Vault to an existing service is subject to minimum term.

It is not currently possible to downgrade from to any PowerCloud Protect service to Managed Service only level during the contract minimum term.

2.6 Connectivity

The customer is responsible for connectivity from their data centres to operate the service where there is an off-site target.

The customer may choose to instruct Synapse360 to procure the connectivity. This is separate and out of scope of the services mentioned in this document.

Supported off-site targets of the service are:

- PowerCloud Protect Products hosted in Synapse 360 datacentre.
- Microsoft Azure Target
- Customer owned or leased datacentres.

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 site-to-site VPN or SD-WAN and it is therefore not a requirement of the service to provision dedicated links.

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 firewalls or routing devices capable and compatible of terminating IPSEC VPN or Azure cloud connectivity. ▪ Provide and fund bandwidth from the customer's data centre at the level required to effectively run the service. ▪ Increase available bandwidth if service requirements grow. ▪ Manage on-site equipment including firewalls. ▪ Patch or upgrade on-site equipment if requested to do so to effectively operate the service. ▪ All ISP charges, support, SLA, management, and contracts
Synapse 360	▪ Run a protection audit that will include bandwidth requirement estimates. ▪ Recommend appropriate bandwidth from customer's site. ▪ Provide bandwidth into the Synapse 360 DC where the service includes hosting. ▪ Configure VPN connectivity in the Synapse 360 DC ▪ Assist with connectivity & security advice to connect to Azure

Remote Management	Connectivity is required for remote management for all PowerCloud Protect products. Management Server ▪ The customer is responsible for ensuring connectivity via secure VPN to all management server IP addresses via LAN/WAN ▪ The customer is responsible for all perimeter devices including switches, routers, firewalls configuration within the customer site required for Synapse 360 access to management servers. ▪ 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:

PowerCloud Protect Operations: Where the customer is not combining with a PowerCloud Protect Backup, Disaster Recovery or Cyber Vault service then the customer must provide all software licenses. The customer must 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.

The licenses to operate and use software & hardware remain the property of the customer during and after termination of the service.

PowerCloud Protect Backup: Backup licensing and support is bundled in the service and is the responsibility of Synapse 360. The service includes the hardware appliances, and we will license the backup for the data and workloads that are specified in scope for the service.

The licenses to operate and use software & hardware remain the property of Synapse 360 during and after termination of the service.

PowerCloud Protect Disaster Recovery: Replication and recovery orchestration licensing and support is bundled in the service and is the responsibility of Synapse 360. The service includes the recovery hardware platform, and we will license appropriately for the data and workloads that are specified in scope for the service.

The licenses to operate and use software & hardware remain the property of Synapse 360 during and after termination of the service.

PowerCloud Protect Backup: Backup licensing and support is bundled in the service and is the responsibility of Synapse 360. The service includes the hardware appliances, and we will license the backup for the data and workloads that are specified in scope for the service.

The licenses to operate and use software & hardware remain the property of Synapse 360 during and after termination of the service.

Software & License Ownership	The service includes all hardware, software licenses and support required to operate the PowerCloud Protect. Vendor support will be maintained by us throughout the service to allow the Synapse 360 MSC to escalate break fix as needed. All software licenses and support are provided for sole use of the service and remain in the control of Synapse 360. At no time will any license transfer in ownership to the customer. Customer supplied and therefore owned licenses or support supplied or obtained outside the PowerCloud Protect contract, used, deployed in or otherwise associated with the service, such as Azure licenses, remain the property of the customer. In that case the responsibility for their renewal, payment, support, and ongoing management remains with the customer at all times.
------------------------------	---

2.8 Hardware Ownership

Hardware Ownership	The use of hardware is rented to the customer under contract 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 MSC Security	The Synapse 360 MSC 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 MSC personnel is performed via the controlled remote desktops that incorporate enterprise anti-virus and anti-malware protection. External email is secured using a 3 rd party gateway. Synapse 360 will ensure the protection tools on the management machines within the MSC are updated regularly.
Encryption	The service is managed via secure VPN from MSC machines only meaning that all traffic between the management client and PowerCloud Protect management tools is encrypted.

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

3. Operating the Service

The service reports directly to the Synapse 360 MSC in the event of a service event or failure. Customers can raise support tickets for events that are not automatically detected by the service monitoring and alerting. Out of hours support tickets can be raised at any time 24/7.

3.1 Operating Synapse 360 PowerCloud Managed Service

Once deployed and live PowerCloud Protect Managed Service is operated entirely by Synapse 360 Managed Service Centre with the exception of requesting contract upgrades that should be done via the account executive.

For all aspects of raising calls, service inclusion, 24/7 support and operating the Foresight service, PowerCloud Protect prospective and existing customers should reference the managed service definition MSD- PowerCloud-Support-xx.docx.

3.2 Requesting Upgrades or Service Extensions

PowerCloud Protect is a flexible and extensible service providing customers with the ability to upgrade throughout the subscription and extend the service term at any time.

The Synapse 360 Managed Service team will advise when an upgrade is recommended or necessary using our predictive monitoring platform and regular reviews, and in addition customers can request a review at any time.

Upgrades or service extensions can be requested at any time either via the Service Delivery Manager during the review process, or by speaking to the aligned account executive.

4 Supporting Services

4.1 Service Monitoring & Alerting

The monitoring solution runs on a cloud platform that is monitored within our MSC. The service is designed to be proactive and reactive to our dedicated team, so no action is normally required from the customer.

Customers can request monitoring or alerting for the service availability occurs to them at no additional cost, and they can request a login to our secure monitoring portal. This additional functionality ensures that the customer's IT team is equally up to date and can share overall responsibility with the Synapse 360 MSC. This is not a requirement of the service.

Additionally, customers can raise tickets via the PowerCloud Support service for user identified events, such as availability or performance, that may not be alerted from within the service.

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 or recommendations for infrastructure improvement.

Frequency	Quarterly. The frequency of the meeting can be varied by request
Attendees	Synapse 360: Service Delivery Manager or Service Owner, optionally the technical architect or aligned technical engineer, and account executive may choose to attend. Customer: Subscription Owner or IT Manager
Format	Remote via Teams/Google meeting / Webex / teleconference or similar. Periodically a face-to-face meeting may be requested.
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 ▪ Changes to the service (requested or suggested) ▪ Options that may be applicable ▪ Recurring issues ▪ Recommended actions ▪ Requests for change
Other Meetings	Additional meetings can be arranged by request including those with 3 rd parties and introduction to other Synapse 360 products or services

5 Service Charges

Synapse 360's default billing period for PowerCloud Protect is monthly in advance from the agreed date that the service is live, as defined by the date where the first customer data is ingested, or the date where the service must be actively managed, backed up, replicated, or monitored. There is generally no additional charge for setting up the service except where agreed remediation is required to configure adjoining networks to be compatible with the service.

Additional Synapse 360 Professional Services that are identified will be performed outside the service.

Contract Term	36-60 Months
Minimum Term	36 Months
Invoice Frequency	Invoicing is monthly in advance
Charging Basis	Charge for the service is calculated on the following: ▪ Hardware & software required to support the service. ▪ Amount of data and workloads to protect. ▪ Data protection levels ▪ Data services required for governance, protection, encryption. ▪ Licenses and support required to support the service. ▪ Bandwidth in the Synapse 360 data centres required to deliver the service
Scaling Basis	The service scales on a monthly basis using the metrics above (charging basis). There may be a lead-time where new hardware or software is required to deliver a requested upgrade to the service, and a new minimum term may be required where the customer is within 12 months of contract renewal.

6 Service Exclusions or Limitations

Exclusions	1. Application deployment design and performance testing 2. Any Protect equipment (hardware, software, or support) directly or indirectly associated with the customer that has not been supplied under the Synapse 360 PowerCloud Protect agreement. 3. Internal Protect in server hardware, desktops or any device not explicitly provided as part of the PowerCloud Protect agreement. 4. Anti-virus, anti-malware licensing, deployment, testing or performance impact mitigation or responsibility. 5. Installation, management, monitoring, setup, upgrade, or licensing of operating systems 6. Installation, management, monitoring, setup, upgrade, or licensing of applications 7. Data owner or any other GDPR defined role or responsibility. 8. Data loss of any kind 9. Licensing, setup, configuration, monitoring, supply, support or warranty of any end user device, PC, laptop, printer 10. Provision, configuration, setup, troubleshooting or support of any kind for home devices and BYOD used to access the service. 11. Licensing, support, or payment to 3rd party of anything not specified explicitly in the service contract. 12. Operating the data centres 13. ISP contract, connection, negotiation, or provision 14. LAN equipment, configuration, uplinks, or any equipment directly or indirectly connected. 15. ISP network termination units (NTU), equipment, connections, or uplinks 16. End user equipment, network cards, connections (unless they are connected to the wi-fi provided in the service) 17. Any network equipment, configuration, provision, configuration, or design not directly covered by this service. 18. Mobile networks, signal strength, quality 19. ISP line interference, delay, jabber, or reliability 20. External firewall configuration, troubleshooting or provision required to install or operate the service (except those that are included in the service) 21. ISP or mobile provider rental, contract, provision, troubleshooting or support costs. 22. Reconfiguration of devices, virtual machines (VMs) end user or mobile devices to work with the service. 23. Replacement of equipment due to mistreatment, unreasonable wear & tear, accidental damage, and theft from customer premises
------------	--

7 Service Levels (SLA) PowerCloud Protect Operations

7.1 SLA Definitions

This section relates to the Business Critical (PowerCloud Support) service levels only. The Synapse 360 PowerCloud Operations 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 MSC
MS-SLA	Operations are measured against customer satisfaction levels and verified by surveys carried out for Synapse 360 by an external company	Customer satisfaction in our operations 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 PowerCloud Protect and invoice the customer on a monthly basis. During this rolling period the customer will continue to enjoy the full features of the PowerCloud Protect and any associated support for as long as they continue to settle the invoice amount.

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

PowerCloud Protect 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 ■ PowerCloud Protect Hardware & software will continue to be available for customer use for as long as they continue to settle the invoiced amount. ■ Synapse 360 PowerCloud Operations configuration, monitoring and troubleshooting will continue with the same SLAs. ■ Some vendor hardware or software support may become unavailable where:
---	---

	○ It is not available to Synapse 360 on a monthly subscription i.e., annualised support will not be purchased during a service continuance. ○ 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
PowerCloud Protect 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 PowerCloud Protect 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 PowerCloud Protect or PowerCloud Platform agreement for a minimum of 36 months. a. Synapse 360 will reassess the environment and propose a new PowerCloud Protect managed service as laid out in this document. b. New hardware and software will be implemented to support the renewed PowerCloud Protect c. Migration planning & testing will commence
Termination of PowerCloud Protect	The customer may choose to terminate part or all of the PowerCloud Protect service at the end of the full term. Synapse 360 will, at best endeavours, assist the customer in the planning and enable migration of Protect away from the PowerCloud Protect. ▪ Where notice of termination is given by the customer Synapse 360 will continue to manage the Protect 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. ▪ The customer will incur costs associated with time and material used to extract data from the solution.
Option to Buy	Synapse 360 will, upon successful negotiation, sell the components of the PowerCloud Protect to the customer and transfer ownership.