

PROACT

G-Cloud 15

Rubrik Managed Backup
Service (BaaS) as a service

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
04/12/2025	Colin Abram	V1	Document Upload



Rubrik Managed Backup Service (BaaS) as a service

Proact provide a range of backup services to provide data protection for customer's data and systems. The service includes the provision of compute, storage and network resources to facilitate the backup of customer data offsite to Proact's data centre. The Backup services provided include:

- Backup as a Service Enterprise – Heterogenous data protection for customer's systems and data
- Backup as a Service Virtual – Data protection for virtual infrastructure
- Backup as a Service O365 – Data protection for customer's Microsoft 365 subscriptions
- Backup as a Service Secure Storage Vault – Data protection for customer's NetApp storage systems

Backup as a Service provides the following deliverables:

- Compute, storage and networking resources required to provide data protection, hosted in a Proact data centre. Where required Proact will provide an onsite disk repository for short term backup retention at the customer's data centre.
- Additional options backup to public cloud
- Provision of software including management to protect data
- Managed backup and recovery
- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring
- Self-service support and self-service monitoring portals
- Management, including break-fix activities, on underlying hardware
- Incident management and resolution
- Problem management
- Change and configuration management
- A named Service delivery manager to co-ordinate delivery and provide regular customer reports

This document contains the following appendices detailing the service definitions for the Backup services:

- [Appendix 1 – Backup as a Service - Enterprise](#)
- [Appendix 2 – Backup as a Service – Virtual](#)
- [Appendix 3 – Backup as a Service – O365](#)
- [Appendix 4 – Backup as a Service – Secure Storage Vault](#)

Appendix 1 - Backup as a Service – Enterprise Service Definition

1.1 - Service Overview

BaaS-E is a backup solution to protect data held within; physical servers, virtual servers, storage arrays, Office 365 and hyperscale public cloud environments.

The Customer is provided with a tenancy within the secure, redundant and highly available BaaS-E environment. All data held within the environment is encrypted for security and retained in a de-duplicated and compressed format.

BaaS-E supports backup of data from multiple Customer locations and can store data in multiple secure locations to provide multiple levels of redundancy and immutability. Proact's Shared Data Vault (SDV) is the default primary storage location.

See the glossary for the definition of acronyms used.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Provide a major incident report, where required. • Provide a change advisory board to review normal, standard, and emergency change requests. • Implement agreed changes to CIs. • Respond to reasonable service requests for relevant information and advice. • Provide reasonable problem management. • Provide incident trend analysis.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems. • Nominate named individuals to engage with Proact on the approval and timing of changes. • Work with Proact to agree predefined actions for common types of incidents.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Standing Charge
Proact shall: • Provide the BaaS platform within Proact's datacentres. • Take appropriate action to restore operation of the BaaS platform in case of outage. • Install and manage anti-virus protection for the BaaS platform. • Provide a dedicated and secure tenancy within the BaaS platform. • Provide all backup software and licenses required to protect the Customer's data.



- Provide Customer access to a secure 'Self Service Restore' portal.
- Encrypt backup data both at-rest and in-flight.
- Create and manage backup policies to meet the Customer's retention and resilience requirements.
- Install and manage backup software on PCDDV backup appliances.
- Manage replication of backup data between source and destination environments.
- Configure immutable time-lock policies for immutable storage targets, upon request.
- Perform data restores for CIs, upon request.
- Monitor backup tasks and respond to failures. Notify the Customer of relevant failures.
- Replicate the master backup server to an alternate DC for redundancy.
- Schedule reports regarding backup job status.
- Perform two scheduled restore tests each year, not overwriting Customer data.
- Assume any recent successful restore will be classed as a successful test restore.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Provide and manage servers/cloud instances required to host software components to backup CIs.
- Provide sufficient compute, network, and storage resource to allow for efficient backup and restore of CIs.
- Provide service accounts and password with privileges to backup and restore the CIs.
- Provide licenses for any application, environment, or SaaS services hosting CIs.
- Provision and manage object storage buckets to host backup storage targets, where required.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Confirm the validity and consistency of restored data.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the BaaS platform. Proact may upgrade the platform at its sole discretion.
- Backup of flat file dumps of databases without the use of application agents.
- Restoring a physical (or virtual) machine to base hardware (bare metal restore).
- Restores that fail or take over 48 hours, due to Customer bandwidth, application, or environment issues.
- Removing backup data related to GDPR right to be forgotten requests.
- Restoring more than 10 out-of-place restore tasks within five working days, such as DR/ransomware restoration.

Managed Dedicated Vault

Proact shall:

- Provide DDV backup appliances, where required.
- Install and manage the OS, AV, and backup software for each DDV appliance.
- Exclude DDV appliances from the Customer Active Directory domain to maintain isolation.

The Customer shall:

- Provide rack space, network ports and cables for any DDV appliances.
- Purchase additional DDV appliances to increase backup capacity, where required.
- Provide network access to the DDV to allow for secure remote management.

Virtual Agent

Proact shall:

- Protect Customer VM backups within a Proact Shared Data Vault.
- Backup VMs at the hypervisor layer (OS consistent with Hypervisor Tools installed).
- Backup public cloud VM instances at the cloud layer (crash consistent).
- Provide granular file level restore upon request.

The Customer shall:

- Remove or reconfigure existing backup or DR tools that impact the service.

Application Agent

Proact shall:

- Provide agents to backup OS and application data in an application consistent format.
- Protect Customer Agent backups within a Proact Shared Data Vault.
- Backup public cloud databases in an application consistent format.
- Truncate application logs were supported and requested.
- Provide granular application level or file level restore upon request.

The Customer shall:

- Remove or reconfigure existing backup or DR tools that impact the service.
- Confirm application consistency is achieved, where supported, by performing test restores.

O365 User
Proact shall:

- Protect Customer O365 backups within a Proact Shared Data Vault.
- Backup Email, OneDrive for Business, Teams, and SharePoint data, where required.

The Customer shall:

- Inform Proact of changes to users/accounts that require backup.
- Ensure users that require backup have a valid O365 subscription assigned.
- Update SaaS service configurations, where required, to ensure BaaS compatibility.
- Convert Public Folders (not supported by Microsoft) to Microsoft 365 Groups where backup is required.

The following elements are out of scope of the service:

- Reduced backup performance due to bandwidth throttling imposed by Microsoft.

Dynamics365 User
Proact shall:

- Protect Customer Dynamics365 backups within a Commvault Cloud Storage tenancy.
- Backup the Dynamics365; Sales, Marketing, Customer Service, and Field Service, where required.

The Customer shall:

- Inform Proact of changes to Dynamics365 services or users/data that require backup.
- Maintain valid licence subscriptions for the Dynamics365 services that require protection.
- Update SaaS service configurations, where required, to ensure BaaS compatibility.

File System & NAS Agent
Proact shall:

- Protect Customer SAN/NAS data backups within a Proact Shared Data Vault.
- Protect Customer Public Object Storage data backups within a Proact Shared Data Vault.
- Protect Customer Operating System File System data backups within a Proact Shared Data Vault.

The Customer shall:

- Remove or reconfigure existing backup or DR tools that impact the service.
- Disable any NAS system AV or create duplicate shares for backup tasks.
- Configure any NAS archiving solution to ignore backup task agent IPs/users.
- When using array vendor backup or DR tools, agree not to truncate application logs or otherwise impact the backup process.

Capacity
Proact shall:

- Provide storage for the backup data within one or more Shared Data Vaults (SDV).
- Provide dual site redundancy by replicating backup data between SDVs at separate sites, upon request.



The Customer shall:

- Request dual site redundancy, where required.

Immutable Capacity

Proact shall:

- Provide storage for backup data within Proact's Immutable Shared Data Vaults (ISDV).
- Manage replication of most recent backups from the SDV to an ISDV held at a separate site.
- Set a time-lock retention policy of a minimum of 14 days to a maximum of 63 days.

Direct Internet Access

Proact shall:

- Provide access to the service via the internet, through a secure firewall.
- Provide internet bandwidth for the transfer of service traffic.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide a network administrator to configure and troubleshoot service traffic.

Clean Room Tier

Proact shall:

- Provide the Clean Room platform within Proact's datacentres.
- Take appropriate action to restore operation of the CR platform in case of outage.
- Provide a dedicated and secure CR tenancy within the platform.
- Assign the CPU, vRAM and Storage capacity for the CR tier contracted.
- Make CR tenancy accessible following Customer access request.
- Provide remote access to VM(s) restored, for the Customer and their IR team.
- Perform each requested Restore Activity for VM(s) up to the vRAM, Storage capacity of the CR tier.
- Isolate VM(s) restored from; the internet, and any external network, to avoid cross contamination.
- Erase VM(s) restored and clean down the CR at Customer request, or after five working days.
- Provide two RAs every 12 months, for the Customer's use.
- Track the quantity of RAs assigned to the Customer and reduce as they are used.
- When a Customer exceeds their RAs assignment, bill the closest RA pack quantity that meets RA usage.
- Schedule a CR restore test once every 12-months, within local business hours. The test will not use an RA.
- During CR restore testing, work with the Customer to agree the VM backup to be tested.
- During CR restore testing, power on VM restored within the CR tenancy.
- Deem testing successful when the recovered VM is remotely accessed by the Customer.
- Change the CR tier assigned, following a written Customer request, as part of a Contract change.
- Automatically expire any unused RAs assigned at the end of the Contract.

The Customer shall:

- Provide 24hours notice of CR access being required, following a ransomware/malware attack.
- Inform Proact of any IR team assigned to the restore validation operation.
- Request RAs be performed and define the VM(s) and backup point in time to be restored.
- Review the VM(s) restored to validate the health of the backup.
- Inform Proact once VM(s) restored has been validated to allow deletion.
- Keep track of the health/infected state of each VM restored.
- Purchase additional RAs, through Restore Activity Packs, where required.
- During testing, work with Proact to agree the VM backup to be tested.
- During testing, utilise remote access to gain access to the OS of the restored VM.
- Provide a written request for changes to the CR tier, where required.
- Hold a valid vendor subscription/license or DR failover rights, for any OS/Application in the tenancy.
- Have an active software assurance contract for any Microsoft applications restored.

Restore Activity Pack	
Proact shall:	Increase the quantity of RAs assigned to the Customer, by the purchased pack quantity.
The Customer shall:	Inform Proact of the quantity of RAs required (RA are available in 5,10,20, & 50 RA packs).

1.2 - Service Level Agreement

1.2.1 - Availability Service Levels

Uptime Commitment – BaaS Platform	Proact will use its reasonable endeavours to achieve an Uptime for the BaaS platform of at least 99.5% of each month. The BaaS platform will be available if the Shared Data Vault and any associated Backup Software located in Proact's data centre responds to Proact's monitoring software.
Uptime Commitment – Comms Internet	Proact will use its reasonable endeavours to achieve an Uptime for the internet connectivity for the service provided to the Customer of at least 99.95% of each month. The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime Commitment – Public Cloud Object Vault	Availability for this service will be dictated by the Service Level Agreement provided by the Customer's own Public Cloud provider. The service availability will be measured according to the Public Cloud provider described measurement. Proact is not accountable for the SLA of the selected Public Cloud provider.
Uptime	The percentage of total possible minutes the service was available during the month: $[(total\ minutes\ in\ month - Downtime) / total\ minutes\ in\ measurement\ period] * 100 = Uptime$
Downtime	The overall number of minutes the service was unavailable during the measurement period. Proact calculates downtime using its standard monitoring tools, the output of which shall be conclusive except in case of manifest error. Downtime excludes any times the service is not available for planned maintenance or reasons beyond Proact's control, as set out in the Standard Terms and Conditions.
Service Credit	If the actual Uptime for this service falls below the Uptime commitment the Customer will be eligible for a Service Credit equal to a percentage of the monthly minimum charges for this service. The relevant percentage is equal to the difference between the actual Uptime achieved and the Uptime commitment, with a minimum of 5% of the relevant monthly charges and a maximum of 50%. A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service.

1.2.2 - Response Time Service Levels

|--|--|



Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: (i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or (ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or (iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change



	advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.3 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Commvault

1.4 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be agents, VMs, NAS file systems, or servers backed up by the service, as set out in the Contract.
Shared Data Vault (SDV)	SDV storage is where backup data is stored within Proact's environment. SDV's store data on high-capacity multi-tenanted storage with double parity RAID to provide redundancy.
Immutable Shared Data Vault (ISDV)	ISDV storage is stored on redundant high-capacity multi-tenanted storage and time locked to prevent modification or deletion of the data by Proact or the Customer until the assigned time lock has expired.
Dedicated Data Vault (DDV)	Where data is stored within the Customer's datacentre, Proact provides a high-capacity DDV hardware appliance to be a local backup target. The DDV appliance is provided, managed and updated by Proact.
Public Cloud Dedicated Data Vaults (PCDDV)	Where data is stored within the Customer's public cloud environment. The Customer will provide a public cloud VM and associated storage to act as a Public Cloud Dedicated Data Vault backup target. The PCDDV appliance VM and its associated OS are provided and managed by the Customer. Proact will manage backup software installed and backup tasks performed on the appliance.
Commvault Cloud Storage (CCS)	Commvault Cloud Storage is a highly resilient multi-tenanted storage held within Commvault's Cloud SaaS Environment. Proact can store data within Commvault's Cloud Storage as the primary backup target for Dynamics365 backups, Office365 Backups or as a secondary backup target for backups held within an SDV.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Clean Room (CR)	The Clean Room is a tenancy within a compute platform hosted in Proact's datacentre that allows virtual machines to be temporarily restored and validated for malware/ransomware infection. The Customer will use this CR in the event of malware/ransomware attack to ensure their VM's are healthy before restoring back to their primary infrastructure. VMs held in a CR are temporary and will be deleted once their health is validated.
Restore Activity (RA)	A Restore Activity is made up of the following steps: Customer requests one or more VM(s) be restored (up to the tier capacity). Proact restore the requested VM(s) into the CR from the SDV Proact make the restored VM(s) accessible to Customer and their IR team Customer, and the IR team, review the restored VM(s) to confirm validity. Proact erase the VM(s) restored, to allow for future restores, since the CR will only hold a single RA. The Clean Room will only hold a single restore activity at a time, to avoid cross contamination. Previous RA's must be completed before a subsequent RA can be performed.
Restore Activity Pack	Multiple restore activities purchased as a bundle, allowing customer's to 'pay as they use'.
Incident Response (IR) team	A cross-functional group of specialists tasked with responding to, and recovering from security incidents, such as a ransomware attack. An IR team may be convened internally by the Customer or contracted as a third party.

Appendix 2 - Backup as a Service – Virtual Service Definition

2.1 Service Overview

Proact's Backup as a Service - Virtual Managed Backup (BaaS-V MB) provides a fully managed backup service to protect data held within; physical servers, virtual servers and hyperscale public cloud environments.

The Customer is provided with a tenancy within the secure, redundant and highly available BaaS-V environment. All data held within the environment is encrypted for security and retained in a de-duplicated and compressed format.

BaaS-V MB can backup data from multiple Customer locations and can store data in multiple secure Proact sites to provide greater redundancy. Proact's Shared Data Vault (SDV) is the default primary storage location. Proact will provide, where required, managed hardware appliances (Dedicated Data Vaults), which will be installed within the Customer's environment. These vaults store local backups of the Customer's data and provide fast restore capabilities.

See the glossary for the definition of acronyms used.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Provide a major incident report, where required. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Respond to reasonable service requests for relevant information and advice. • Provide reasonable problem management. • Provide incident trend analysis.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems. • Nominate named individuals to engage with Proact on the approval and timing of changes. • Work with Proact to agree predefined actions for common types of incidents.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Standing Charge
Proact shall: • Provide the BaaS platform within Proact's datacentres. • Take appropriate action to restore operation of the BaaS platform in case of outage. • Install and manage anti-virus protection for the BaaS platform.



- Provide an encrypted tunnel over the internet to secure service traffic.
- Provide all backup software and licenses required to protect the Customer's data.
- Install and manage master server(s), deployed within the Customer's VM environment.
- Provide Customer access to secure 'Self Service Restore'.
- Encrypt backup data both at-rest and in-flight.
- Create and manage backup policies to meet the Customer's retention and resilience requirements.
- Install and manage backup software on PCDDV backup appliances.
- Manage replication of backup data between source and destination environments.
- Retain deleted backup data for 7 days to allow recovery, upon request, following erroneous or malicious acts.
- Perform data restores for CIs, upon request.
- Monitor backup tasks and respond to failures. Notify the Customer of relevant failures.
- Replicate the master backup server and associated encryption keys, to a Proact SDV for redundancy.
- Schedule reports regarding backup job status.
- Perform two scheduled restore tests each year, not overwriting Customer data.
- Assume any recent successful restore will be classed as a successful test restore.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Provide and manage servers/cloud instances required to host software components to backup CIs.
- Provide sufficient compute, network, and storage resource to allow for efficient backup and restore of CIs.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Provide 'Service Accounts' and password with privileges to backup and restore the CIs.
- Provide licenses for any application, environment, or SaaS services hosting CIs.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Confirm the validity and consistency of restored data.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the BaaS platform. Proact may upgrade the platform at its sole discretion.
- Backup of flat file dumps of databases without the use of application agents.
- Restoring a physical (or virtual) machine to base hardware (bare metal restore).
- Restores that fail or take over 48 hours, due to Customer bandwidth, application, or environment issues.
- Removing backup data related to GDPR right to be forgotten requests. Proact can offer professional services to assist with per Customer reasonable requirements.

Managed Dedicated Vault

Proact shall:

- Provide DDV backup appliances, where required.
- Install and manage the OS, AV, and backup software for each DDV appliance.
- Exclude DDV appliances from the Customer Active Directory domain to maintain isolation.

The Customer shall:

- Provide rack space, network ports and cables for any DDV appliances.
- Purchase additional DDV appliances to increase backup capacity, where required.
- Provide network access to the DDV to allow for secure remote management.

Virtual Agent

Proact shall:

- Protect Customer VM backups within a Proact Shared Data Vault.
- Backup VMs at the hypervisor layer (OS consistent with Hypervisor Tools installed).
- Provide granular file level restore upon request.

Public Cloud Virtual Agent

Proact shall:

- Protect Customer Agent backups within a Proact Shared Data Vault.
- Provide agents to backup public cloud VMs in and OS and application consistent format.
- Backup public cloud databases in an application consistent format.
- Truncate application logs were supported and requested.
- Provide granular application level or file level restore upon request.

The Customer shall:

- Remove or reconfigure existing backup or DR tools that impact the service.
- Confirm application consistency is achieved, where supported, by performing test restores.

Physical Agent

Proact shall:

- Provide agents to backup OS and application data in an application consistent format.
- Backup public cloud databases in an application consistent format.
- Truncate application logs were supported and requested.
- Provide granular application level or file level restore upon request.

The Customer shall:

- Remove or reconfigure existing backup or DR tools that impact the service.
- Confirm application consistency is achieved, where supported, by performing test restores.

Capacity

Proact shall:

- Provide storage for the backup data within one or more Shared Data Vaults (SDV).
- Provide dual site redundancy by replicating backup data between SDVs at separate sites, upon request.

The Customer shall:

- Request dual site redundancy, where required.

Direct Internet Access

Proact shall:

- Provide access to the service via the internet, through a secure firewall.
- Provide internet bandwidth for the transfer of service traffic.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide a network administrator to configure and troubleshoot service traffic.

1.5 - Service Level Agreement

1.5.1 - Availability Service Levels

Uptime Commitment – BaaS Platform	Proact will use its reasonable endeavours to achieve an Uptime for the BaaS platform of at least 99.5% of each month. The BaaS platform will be available if the Shared Data Vault and any associated Backup Software located in Proact's data centre responds to Proact's monitoring software.
Uptime Commitment – Comms Internet	Proact will use its reasonable endeavours to achieve an Uptime for the internet connectivity for the service provided to the Customer of at least 99.95% of each month. The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime	The percentage of total possible minutes the service was available during the month: $[(\text{total minutes in month} - \text{Downtime}) / \text{total minutes in measurement period}] * 100 = \text{Uptime}$
Downtime	The overall number of minutes the service was unavailable during the measurement period. Proact calculates downtime using its standard monitoring tools, the output of which shall be conclusive except in case of manifest error. Downtime excludes any times the service is not available for reasons beyond Proact's control as set out in the Standard Terms and Conditions.
Service Credit	If the actual Uptime for this service falls below the Uptime commitment the Customer will be eligible for a Service Credit equal to a percentage of the monthly minimum charges for this service. The relevant percentage is equal to the difference between the actual Uptime achieved and the Uptime commitment, with a minimum of 5% of the relevant monthly charges and a maximum of 50%. A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service.

1.5.2 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal, and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: (i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or (ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or



	(iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan.



	If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working hours for changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.6 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Veeam

1.7 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be agents or VMs backed up by the service, as set out in the Contract.
Shared Data Vault (SDV)	Shared Data Vault storage is stored within Proact's environment. SDVs store data on high-capacity multi-tenanted storage, with double parity RAID to provide redundancy.
Dedicated Data Vault (DDV)	Where data is stored within the Customer's datacentre, Proact provides a high-capacity Dedicated Data Vault hardware appliance to be a local backup target. The DDV appliance is provided, managed, and updated by Proact.
Public Cloud Dedicated Data Vaults (PCDDV)	Where data is stored within the Customer's public cloud environment. The Customer will provide a public cloud VM and associated storage to act as a Public Cloud Dedicated Data Vault backup target. The PCDDV appliance VM and its associated OS are provided and managed by the Customer. Proact will manage backup software installed and backup tasks performed on the appliance.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.

Appendix 3 - BaaS-O365 Service Definition

3.1 Service Overview

Backup as a Service for Office365 (BaaS-O365) provides a backup solution for business data running within Microsoft O365 Cloud SaaS Service.

Proact will deliver a fully managed service that will integrate with O365 and provide an independent backup of business data external to O365, to allow for point in time data protection, as well as allowing access to business data in the event that O365 services are not available.

See the glossary for the definition of acronyms used.

General Service Deliverables

Proact shall:

- Provide a service desk and customer support portal to report and update incidents, change requests and escalations.
- Provide a Service Platform.
- Provide service delivery management.
- Maintain documentation of the service configuration.
- Maintain a CMDB listing for all CIs.
- Respond to Service Platform alerts and events and notify the Customer of relevant incidents.
- Coordinate any product vendor involvement necessary.
- Take appropriate action to restore operation of the Service Platform in case of outage.
- Provide a major incident report, where required.
- Provide a change advisory board to review normal, standard, and emergency change requests.
- Subject to agreement, join the Customer's change advisory board, for relevant changes.
- Implement agreed changes to CIs.
- Respond to reasonable service requests for relevant information and advice.
- Provide reasonable problem management.
- Provide incident trend analysis.

The Customer shall:

- Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level.
- Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone.
- Assist with any systems or applications not under Proact's management.
- Respond to requests for information/actions within five working days. Inactive incidents may be closed.
- Resolve health issues on customer-managed systems.
- Nominate named individuals to engage with Proact on the approval and timing of changes.
- Work with Proact to agree predefined actions for common types of incidents.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Standing Charge

Proact shall:

- Provide the BaaS platform within Proact's datacentres.
- Take appropriate action to restore operation of the BaaS platform in case of outage.
- Install and manage anti-virus protection for the BaaS platform.
- Provide a dedicated and secure tenancy within the BaaS platform.
- Provide all backup software and licenses required to protect the Customer's data.
- Provide access to the service via the internet, through a secure firewall.
- Provide Customer access to a secure 'Self Service Restore' portal.
- Encrypt backup data during transfer to the BaaS platform.
- Create and manage backup policies to meet the Customer's retention and resilience requirements.

- Manage replication of backup data between O365 and BaaS-O365 platform.
- Perform data restores for CIs, upon request.
- Monitor backup tasks and respond to failures. Notify the Customer of relevant failures.
- Schedule reports regarding backup job status.
- Perform two scheduled restore tests each year, not overwriting Customer data.
- Assume any recent successful restore will be classed as a successful test restore.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Provide service accounts and password with privileges to backup and restore the CIs.
- Provide licenses for any application, environment, or SaaS services hosting CIs.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Provide a network administrator to configure and troubleshoot service traffic.
- Confirm the validity and consistency of restored data.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the BaaS platform. Proact may upgrade the platform at its sole discretion.
- Restores that fail or take over 48 hours, due to Customer bandwidth, application, or environment issues.
- Removing backup data related to GDPR right to be forgotten requests. Proact can offer professional services to assist with per Customer reasonable requirements.

O365 User (Including Storage)

Proact shall:

- Protect Customer O365 backups within one or more Proact REPOs.
- Backup: Email, OneDrive for Business, Teams, and SharePoint data, where required.
- Provide internet bandwidth for the transfer of service traffic.
- Provide storage for each user in line with the O365 User Capacity.
- Validate the Customer's O365 User Capacity periodically.
- Apply capacity-based charges, where the Customer exceeds, or will exceed O365 User Capacity, as part of a Contract change.

The Customer shall:

- Inform Proact of changes to users/accounts that require backup.
- Ensure users that require backup have a valid O365 subscription assigned.
- Where O365 'two factor authentication' is in place, provide 2FA access to assist with the restore.
- Update SaaS service configurations, where required, to ensure BaaS compatibility.
- Convert Public Folders to Microsoft365 Groups and inform Proact, where backup is required.
- Inform Proact where the customer exceeds, or will exceed O365 User Capacity.

The following elements are out of scope of the service:

- Reduced backup or restore performance due to bandwidth throttling imposed by Microsoft.

O365 User (Excluding Storage)

Proact shall:

- Perform Customer O365 backups within one or more Proact REPOs.
- Backup: Email, OneDrive for Business, Teams, and SharePoint data, where required.
- Provide internet bandwidth for the transfer of service traffic.

The Customer shall:

- Inform Proact of changes to users/accounts that require backup.
- Ensure users that require backup have a valid O365 subscription assigned.
- Where O365 'two factor authentication' is in place, provide 2FA access to assist with the restore.
- Update SaaS service configurations, where required, to ensure BaaS compatibility.
- Convert Public Folders to Microsoft365 Groups and inform Proact, where backup is required.

The following elements are out of scope of the service:



- Reduced backup or restore performance due to bandwidth throttling imposed by Microsoft.

O365 Capacity

Proact shall:

- Provide storage for the backup data within one or more Proact REPOs

1.8 - Service Level Agreement

1.8.1 - Availability Service Levels

Uptime Commitment – BaaS Platform	Proact will use its reasonable endeavours to achieve an Uptime for the BaaS platform of at least 99.5% of each month. The service will be available if the Customer's REPOs and associated backup server located in Proact's data centre respond to Proact's monitoring software and if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime Commitment – Comms Internet	Proact will use its reasonable endeavours to achieve an Uptime for the internet connectivity for the service provided to the Customer of at least 99.99% of each month. The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime	The percentage of total possible minutes the service was available during the month: $[(\text{total minutes in month} - \text{Downtime}) / \text{total minutes in measurement period}] * 100 = \text{Uptime}$
Downtime	The overall number of minutes the service was unavailable during the measurement period. Proact calculates downtime using its standard monitoring tools, the output of which shall be conclusive except in case of manifest error. Downtime excludes any times the service is not available for planned maintenance or reasons beyond Proact's control, as set out in the Standard Terms and Conditions.
Service Credit	If the actual Uptime for this service falls below the Uptime commitment the Customer will be eligible for a Service Credit equal to a percentage of the monthly minimum charges for this service. The relevant percentage is equal to the difference between the actual Uptime achieved and the Uptime commitment, with a minimum of 5% of the relevant monthly charges and a maximum of 50%. A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service.

1.8.2 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is:

	(i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or (ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or (iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope and which cannot wait for review and approval from the CAB. Where



	there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.9 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Veeam

1.10 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be Office365 user accounts backed up by the service, as set out in the Contract.
Data Centre (DC)	A facility that provides network, compute, and storage infrastructure for the Customers use, outside of their internal network. This environment is designed and maintained to ensure high security and high availability.
Dedicated Backup Repository (REPO)	Dedicated backup repositories (REPOs) are held within a Proact's datacentre to store the Customer's backup data. A Customer may have one or more REPOs depending on their storage requirements. REPO data is stored on high-capacity, low-performance storage, with double parity RAID to provide redundancy.



Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
O365 User Capacity	Proact will provide 30GB of storage per user, on average, over the term of the Contract.

Appendix 4 - Backup as a Service – Secure Storage Vault Service Definition

4.1 Service Overview

Backup as a Service - Secure Storage Vault (BaaS-SSV) is an offsite backup vault for Customers who have NetApp ONTAP storage, run ONTAP storage in the cloud, or utilise ONTAP storage within Proact's Datacentres.

The offsite backup vault is hosted in a Proact datacentre and acts as a replication target for volumes, LUNs, and Storage Virtual Machines (SVMs) hosted on the Customer's existing ONTAP storage. Where the ONTAP storage is also hosted within a Proact datacentre or within an existing Proact managed service (such as PHC or PMCP), BaaS-SSV will replicate to an alternate Proact datacentre to ensure the data is offsite. Replication will be performed using either NetApp SnapMirror or SnapVault technology.

Proact will monitor all backups being sent to the Secure Storage Vault and perform restore tasks on behalf of the Customer.

See the glossary for the definition of acronyms used.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Provide a major incident report, where required. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Respond to reasonable service requests for relevant information and advice. • Provide reasonable problem management. • Provide incident trend analysis.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on Customer-managed systems. • Nominate named individuals to engage with Proact on the approval and timing of changes. • Work with Proact to agree predefined actions for common types of incidents.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Backup Storage
Proact shall: • Provide the BaaS platform within Proact's datacentres.



- Take appropriate action to restore operation of the BaaS platform in case of outage.
- Provide replication software and licenses on the BaaS platform.
- Provide an encrypted tunnel over the internet to secure service traffic.
- Encrypt backup data during transfer to the BaaS platform.
- Provide a dedicated SSV for the Customer within one or more Proact's datacentres.
- Provide a replication target for each CI replicated from the Customer's ONTAP array.
- Encrypt replication targets at Proact, upon request. Proact will hold the encryption keys.
- Retain the de-duplication and compression setting of each source CI within the replication target.
- Provide both capacity and performance tiers of storage for the replication targets.
- Provide dual site redundancy by replicating backup data to two SSVs at separate sites, upon request.
- Work with the Customer to initiate replication of source CIs and troubleshoot replication problems.
- Create and manage backup policies to meet the Customer's retention and resilience requirements.
- Manage replication of backup data between source and destination environments.
- Monitor backup tasks and respond to failures. Notify the Customer of relevant failures.
- Perform two scheduled restore tests each year, not overwriting Customer data.
- Assume any recent successful restore will be classed as a successful test restore.
- Perform data restores for CIs, upon request.
- Work with the Customer meet the requirements for each restore and use the optimal approach available.
- Schedule reports regarding backup job status.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Define CIs that require backup, and the target storage tier required, and inform Proact of changes.
- Provide ONTAP arrays, instances or software appliances, hosting data, that requires backup.
- Provide ONTAP software and licenses to enable backup replication.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Inform Proact of CIs that require encryption at-rest within the replication target.
- Request dual site redundancy for replication targets, where required.
- Manage snapshots on the source ONTAP system to define recovery points replicated to Proact.
- Remove or reconfigure existing backup or DR tools that impact the service.
- Manage NetApp SnapCenter, or 3rd applications, to support application consistent snapshots.
- Work with Proact to initiate backup replication and troubleshoot replication problems.
- Provide sufficient compute, network, and storage resource to allow for efficient backup and restore of CIs.
- Provide 'Service Accounts' and password with privileges to backup and restore the CIs.
- Provide licenses for any application, environment, or SaaS services hosting CIs.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Confirm the validity and consistency of restored data.
- Confirm application consistency is achieved, where supported, by performing test restores.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the BaaS platform. Proact may upgrade the platform at its sole discretion.
- Use of SSV replication targets for DR recovery/failover. DRaaS is available for DR protection.
- Restores that fail or take over 48 hours, due to Customer bandwidth, application, or environment issues.
- Removing backup data related to GDPR right to be forgotten requests. Proact can offer professional services to assist with per Customer reasonable requirements.

Direct Internet Access

Proact shall:

- Provide access to the service via the internet, through a secure firewall.
- Provide internet bandwidth for the transfer of service traffic.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide a network administrator to configure and troubleshoot service traffic.



1.11 - Service Level Agreement

1.11.1 - Availability Service Levels

Uptime Commitment – BaaS Platform	Proact will use its reasonable endeavours to achieve an Uptime for the BaaS platform of at least 99.5% of each month. The BaaS platform will be available if the Secure Storage Vault and any associated ONTAP Software located in Proact's data centre responds to Proact's monitoring software.
Uptime Commitment – Comms Internet	Proact will use its reasonable endeavours to achieve an Uptime for the internet connectivity for the service provided to the Customer of at least 99.95% of each month. The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime Commitment – Public Cloud Object Vault	Availability for this service will be dictated by the service level agreement provided by the Customer's own Public Cloud provider. The service availability will be measured according to the Public Cloud provider described measurement. Proact is not accountable for the SLA of the selected Public Cloud provider.
Uptime	The percentage of total possible minutes the service was available during the month: $[(\text{total minutes in month} - \text{Downtime}) / \text{total minutes in measurement period}] * 100 = \text{Uptime}$
Downtime	The overall number of minutes the service was unavailable during the measurement period. Proact calculates downtime using its standard monitoring tools, the output of which shall be conclusive except in case of manifest error. Downtime excludes any times the service is not available for planned maintenance or reasons beyond Proact's control, as set out in the Standard Terms and Conditions.
Service Credit	If the actual Uptime for this service falls below the Uptime commitment the Customer will be eligible for a Service Credit equal to a percentage of the monthly minimum charges for this service. The relevant percentage is equal to the difference between the actual Uptime achieved and the Uptime commitment, with a minimum of 5% of the relevant monthly charges and a maximum of 50%. A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service.

1.11.2 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: (i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or



	(ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or (iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there

	is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working hours for changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.12 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
NetApp

1.13 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be volumes, LUNs or NetApp Storage Virtual Machines (SVMs) backed up by the service, as set out in the Contract.
Secure Storage Vault (SSV)	An SSV is a ONTAP replication target, dedicated to the Customer, stored within Proact's environment. The SSV will receive backup ONTAP volumes from the Customer's ONTAP array. SSVs provide multi-tenanted storage with multiple tiers, offering both performance and high-capacity RAID storage.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.