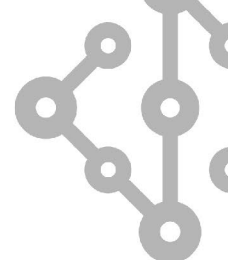




SysGroup

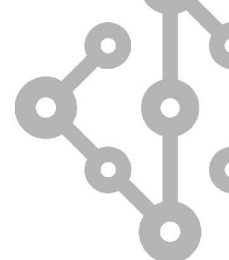
SysGroup Backup as a Service

Service Definition Document

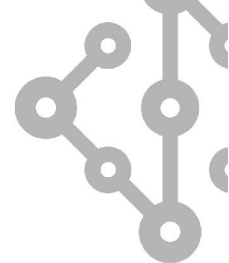


Contents

Document Control	4
Introduction	5
Definitions and Sign-Off	6
Parties and Definitions	6
Revisions to the Document	6
SysGroup Sign-Off	6
Customer Sign-Off	7
Contract Period	7
In Scope Services	8
BaaS Description	8
Integration & Interoperability	9
Onboarding & Offboarding Framework	10
BaaS Roles and Responsibilities	13
BaaS Options	14
BaaS Platform Benefits	15
BaaS Retention Options	15
BaaS Recovery Testing	16



Customer Access	16
Incident Management.....	17
Operations Team Introduction	17
Personal Security Controls	17
Incident Reporting.....	18
Escalation Path	19
Service Constraints.....	20
Out of Scope	21
Service Levels	22
CHANGE/SERVICE REQUEST SLA's:	23
Service Review Meetings.....	24
Call Frequency	24
Complaints Procedure.....	24
Change Management	25
Change Control Notification.....	25
Appendix A – Contact Information	26
Approved Service Callers from CUSTOMER.....	27



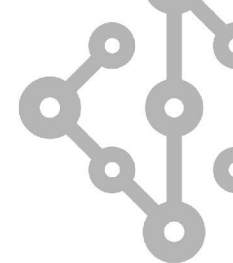
Document Control

Version Control

Created	01/01/25
Author	Kevin Johnson
Author's Position	Platform Lead – Data Protection

Document History

Date	Name	Change Description
17/12/25	Kevin Johnson	V3



Introduction

The purpose of this document is to act as the Service Catalogue for the SysGroup Backup as a Service (BaaS) offering, to which both parties are in full agreement. This Service Catalogue serves as a central repository of information including, but not limited to, general contact details, Service Level Agreements (SLAs), incident logging procedures, service descriptions, monitoring systems and escalation paths.

SysGroup support processes are aligned to ITIL standards for best practice in IT Service Management. Our approach, based on ITIL best practice, ensures that customers receive high-quality Incident, Problem and Change Management, all managed centrally by our fully trained and dedicated Operations Team.

SysGroup Backup-as-a-Service (BaaS) is a fully managed data-protection service powered by the Rubrik Security Cloud. The service provides secure, immutable backup capabilities alongside cyber-resilient recovery, continuous monitoring and full lifecycle management of backup and recovery operations. Key features of the service include:

- Immutable, ransomware-resistant backups
- Secure protection of enterprise, cloud, SaaS and unstructured data
- Automated retention, encryption and off-site copies
- Threat detection, anomaly detection and threat hunting
- Rapid recovery of virtual machines, applications, databases and file systems
- Disaster Recovery orchestration and validation
- 24/7 UK-based Operations Centre support
- Quarterly recovery tests and reporting
- Compliance reporting for GDPR, PCI-DSS and ISO 27001

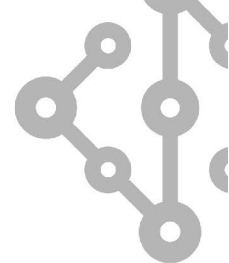
SysGroup support processes are aligned to the ITIL standards for best practice in IT Service Management. Our approach, based on ITIL best practice, ensures that customers will receive high-quality Incident, Problem and Change Management, managed centrally by our fully trained and dedicated Operations team.

Operations

The SysGroup Operations Team is responsible for supporting your BaaS service. The Operations Team will log and progress faults and technical queries. They will issue you with a reference number and keep you informed on the progress of your query. The Operations Team will operate within the agreed service levels.

Pro-active Approach

SysGroup has a pro-active approach to delivery of this service and will inform CUSTOMER with a notification and request to engage when a new BaaS upgrade with functionality relevant to CUSTOMER, is available. Similarly, if SysGroup is made aware of any BaaS issues via their relationship that are relevant to CUSTOMER, we will notify you to agree the next steps.



Definitions and Sign-Off

Parties and Definitions

This document has been agreed between the following parties:

(1) SysGroup, whose registered office is at 55 Spring Gardens, Manchester M2 2BY, hereby referred to throughout this document as "SysGroup"

and

(2) CUSTOMER, registered in England and Wales (company number XXXXXXXX) with its registered office at ADDRESS, ADDRESS 2, CITY, POST CODE hereby referred to throughout this document as "CUSTOMER"

Revisions to the Document

SysGroup will release a revised handbook should CUSTOMER inform them of any changes to the table shown in Appendix A. Changes to the Appendix will not require formal sign-off from either party. However, should SysGroup release a revised handbook following any changes to section 3 to 5, sign-off will be sought from CUSTOMER and SysGroup.

SysGroup Sign-Off

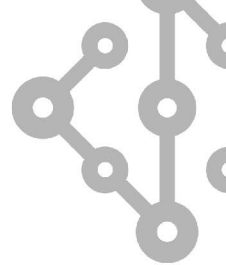
Upon sign-off of this document, SysGroup commits to providing the services as outlined in sections 3 to 7 of this handbook in accordance with the agreed timescales.

Signed on behalf of SysGroup PLC:

Name: Simon Kirkup

Position: Chief Technical Officer

Signature:



Customer Sign-Off

Upon sign-off of this document, CUSTOMER commits to following the processes outlined in sections 3 to 5 of this handbook. CUSTOMER understands that failure to comply may result in a delay and the agreed timescales will not apply.

Signed on behalf of CUSTOMER:

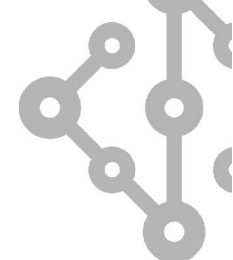
Name:

Position:

Signature:

Contract Period

The period of support for this service is from <Start Date> to <End Date>



In Scope Services

BaaS Description

BaaS provides the capability to back up data from a customer site to SysGroup's data centre, with three different architectures available depending on customer requirements. The service is delivered as a remotely managed solution, with backup appliances deployed on the customer site where required by the chosen architecture. All backup, monitoring and restore operations are delivered online through the SysGroup and Rubrik platforms, ensuring secure and efficient data protection. Support is provided remotely by SysGroup's 24/7 Operations Team, enabling continuous oversight and rapid response to backup or recovery needs.

Category	Description
BaaS – Local Only	Local Backup server/appliance with managed service wrap around
BaaS – Local with Remote Offsite Copy	Local Backup server/appliance with Remote Offsite Copy
BaaS – Local with Offsite Warm Standby	Replicate VM's/Workloads for low RTO/RPO

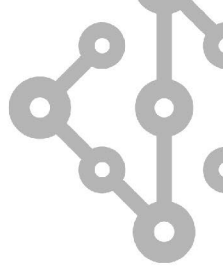
SysGroup's Backup as a Service (BaaS) delivers measurable improvements across cyber resilience, operational efficiency, compliance and overall service quality. By combining immutable backup technology, automation and 24/7 managed support, the service is designed to reduce risk, improve recoverability and streamline backup operations for the customer. Key benefits include:

Cyber Resilience

- Faster recovery times (up to 70% improvement reported)
- Reduced downtime (restoration in minutes, not hours)
- Protection against ransomware reinfection
- Guaranteed recoverability through immutable storage

Operational Efficiency

- Reduced operational overhead (40% reduction reported)
- Predictable monthly billing
- Consolidation of backup and cyber tools into one platform

**Compliance**

- Audit-ready reporting for major frameworks
- UK-based hosting ensuring data sovereignty
- Full visibility and logging for compliance checks

Service Quality

- Continuous monitoring and proactive communication
- Quarterly recovery testing
- Outcome-focused managed service
- Defined SLAs and guaranteed response times

Integration & Interoperability

SysGroup BaaS can protect the following workloads:

Physical:

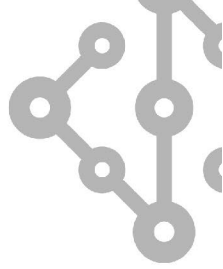
- Windows Server
- Unix/Linux
- Oracle Solaris
- Oracle Database
- PostgreSQL
- SAP HANA
- MS SQL Server

Virtual:

- VMware
- Nutanix
- Hyper-V

Cloud & SaaS

- AWS
- Azure
- GCP
- Oracle Cloud
- Microsoft 365



Onboarding & Offboarding Framework

Onboarding:

Objectives: establish scope, authority, and compliance baseline.

Activities

- Service agreement & SLA sign-off
- Data classification & compliance requirements (GDPR, HIPAA, ISO, etc.)
- Define RPO / RTO
- Identify in-scope systems & applications
- Confirm data residency and retention requirements
- Nominate customer technical & security contacts

Outputs

- Signed contract & SLA
- Approved backup scope
- Governance contacts matrix

Technical Onboarding:

Objectives: enable secure connectivity and backup capability.

Activities

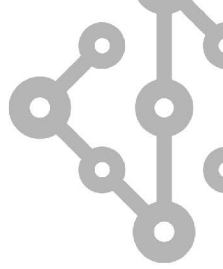
- Create customer tenant / vault
- Configure encryption (BYOK or provider-managed keys)
- Establish network connectivity (VPN, private endpoint, firewall rules)
- Configure service accounts / API access
- Deploy backup agents or enable agentless integrations
- Apply least-privilege access controls (RBAC)

Provider Responsibilities

- Platform provisioning
- Security baseline enforcement
- Initial configuration support

Customer Responsibilities

- Access approvals
- Credential provisioning
- Network changes

**Backup Policy Configuration:**

Objectives: ensure backups meet business and compliance needs.

Activities

- Define schedules (daily, hourly, continuous)
- Set retention policies (short/long-term)
- Configure backup types (full, incremental, snapshot)
- Enable immutability / ransomware protection (if applicable)
- Configure monitoring and alerting

Outputs

- Documented backup policies
- Approved retention schedules

Validation & Acceptance:

Objectives: confirm backups and restores work as expected.

Activities

- Initial backup execution
- Backup success verification
- Test restore (file-level or full system)
- Performance validation against RPO/RTO
- Customer sign-off

Outputs

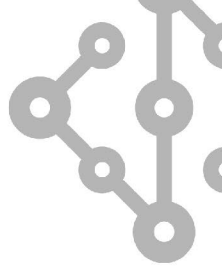
- Acceptance sign-off
- Onboarding completion report

Operational Handover:

Objectives: transition to steady-state service.

Activities

- Provide operational documentation
- Confirm support escalation paths
- Schedule regular reporting
- Define change management process
- Agree restore request workflow

**Offboarding:**

Objectives: protect data integrity and compliance during exit.

Activities

- Confirm termination date
- Identify data to be retained, transferred, or deleted
- Validate legal hold requirements
- Agree export format and timeline
- Obtain written authorization for data deletion

Critical Control

- No data deletion without explicit customer approval

Data Export / Transition (If required):

Objectives: ensure continuity of protection.

Activities

- Perform final full backup
- Export data securely (encrypted transfer)
- Verify data completeness and integrity
- Support migration testing (if contracted)

Outputs

- Export confirmation
- Transfer logs

Data Deletion & Secure Disposal:

Objectives: ensure compliant data destruction.

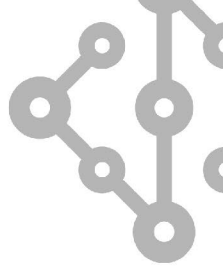
Activities

- Execute secure deletion per policy
- Destroy encryption keys (if applicable)
- Remove customer tenants and credentials
- Revoke access rights
- Update asset and data registers

Outputs

- Certificate of Data Destruction (where applicable)
- Offboarding confirmation report

Account & Service Closure:

**Activities**

- Disable monitoring and alerting
- Close billing
- Archive audit logs per retention policy
- Final SLA and usage report

BaaS Roles and Responsibilities

As a managed service provider SysGroup's responsibility is:

Responsibilities

- Backup platform provisioning & management
- Automated backup execution per agreed schedules
- Secure storage (encryption at rest & in transit)
- Monitoring, alerting & reporting
- Backup integrity checks and success verification
- Disaster recovery support (restore assistance)
- SLA management (availability, success rates)

Accountable for

- Backup service availability
- Secure handling of backed-up data
- Meeting contracted SLAs

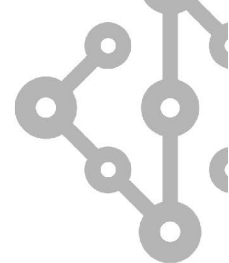
Customer responsibility is:

Responsibilities

- Data ownership & classification
- Defining backup scope (systems, apps, retention, RPO/RTO)
- Ensuring data accuracy at source
- Approving retention and deletion policies
- Initiating and validating restore requests
- Meeting regulatory obligations (GDPR, HIPAA, ISO, etc.)

Accountable for

- Data compliance and legal retention
- Business continuity requirements
- Authorization of restores and access



BaaS Options

BaaS Endpoint

Data Protection – Protects endpoint data from cyberattacks, malicious insiders and operational disruptions by using automated, immutable, air-gapped and access-controlled backups. This ensures user devices can be recovered quickly and securely in the event of loss, compromise or failure.

BaaS Foundation:

Data Protection – Provides enterprise-grade protection for cloud, SaaS and unstructured data using automated, immutable, air-gapped and access-controlled backups designed to defend against cyberattacks and operational disruptions.

Mass Recovery – Enables rapid restoration of business operations by recovering applications, databases, files or objects at scale, significantly reducing downtime.

Data Security Command Centre – Identifies security gaps and data-risk exposure, offering actionable insights and recommendations to strengthen the organisation's data-security posture.

BaaS Standard:

As BaaS foundation with the addition of:

Anomaly Detection – Uses machine learning to detect suspicious deletions, modifications or encryptions within backup sets, helping determine the scope and impact of cyberattacks.

Threat Monitoring – Automatically identifies indicators of compromise within backup data by leveraging an up-to-date feed of global threat intelligence.

Threat Hunting – Analyses historical data to identify malware activity, supporting digital forensics and helping prevent reinfection.

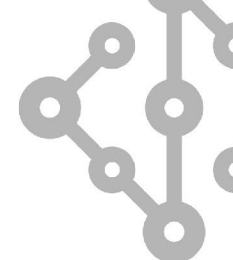
Threat Containment – Quarantines infected backup data to ensure safe and rapid recovery during cyber incidents.

BaaS Enterprise:

As BaaS Standard with the addition of:

Sensitive Data Monitoring – Identifies what types of sensitive data exist and where they reside, helping organisations reduce exposure and meet compliance requirements.

Exfiltration-Risk Analysis – Assesses sensitive-data exposure and evaluates the risk of data exfiltration, improving data-governance and regulatory posture.



BaaS Enterprise Plus:

As BaaS Enterprise with the addition of:

Cyber Recovery – Conducts periodic recovery-validation exercises, attack simulations and other resilience assessments to ensure that recovery processes are proven, secure and effective during real-world incidents.

The BaaS offering is available as a 1-year or 3-year subscription, supported by a predictable monthly billing model that provides clear cost forecasting. Organisations can achieve further savings through the consolidation of backup, cyber recovery and security-visibility tools into a single platform. Pricing varies depending on the selected BaaS tier—Endpoint, Foundation, Standard, Enterprise or Enterprise Plus—as well as the chosen architecture. SME input will be required to finalise the pricing table for G-Cloud, but all service options outlined above can be purchased under either a 1-year or 3-year subscription commitment.

BaaS Platform Benefits

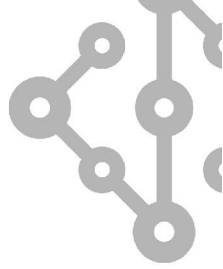
Rubrik's Zero Trust Architecture underpins the entire BaaS offering, delivering a modern security model that provides up to 100x faster cyber recovery when compared to legacy backup tools. All backups are fully immutable and protected from deletion, modification or encryption, ensuring that recovery data remains uncompromised even during advanced cyber incidents. The platform combines Data Security Posture Management (DSPM) with cyber-recovery capabilities in a single solution, supported by SysGroup-certified Rubrik engineers and ISO-qualified lead auditors. With a UK-based 24/7 operations team, customers benefit from continuous monitoring and expert response. SysGroup also offers a Risk Reversal Guarantee, ensuring that if recoveries do not perform as expected, any issues are resolved at no additional cost. The service is designed specifically for mid-sized and growing organisations, providing tailored protection and clear, audit-ready compliance reporting.

BaaS Retention Options

Below are the standard retentions offered with SysGroup BaaS:

Category	Available Retention Period
BaaS – Local Only	14-day local retention
BaaS – Local with Remote Offsite Copy	14-day local retention and 30-day offsite copy retention
BaaS – Local with Offsite Warm Standby	14-day local retention. RTO and RPO of less than 15 minutes

Retention periods can be increased if required by customer.



BaaS Recovery Testing

Restore testing will be carried out once a quarter with results sent to the customer for verification.

Customer can request restore testing be carried out at any time as part of a change request outlined in section 5.5 of this document.

Customer Access

Customers can access the BaaS service via a web portal. SysGroup BaaS uses role-based access meaning every user logs in with a role that defines exactly what a user can see and do in the system.

SysGroup BaaS provides built-in roles, although custom roles can be defined by customers is required:

Administrator

- Full access to all Rubrik features
- Create/delete SLAs, manage clusters, run backups/ restores
- Manage users & roles

Backup Admin / Operator

- Can run backup/restore tasks
- Limited configuration management
- Cannot modify cluster-level settings

Read-Only

- Can view objects, SLAs, cluster status
- Cannot run backup/restore operations
- Typically used for audits and reporting

Custom Roles

- Permissions tailored per team or customer

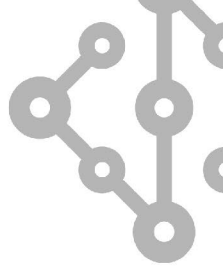
Accessibility

The web portal is designed to meet **WCAG 2.1 AA accessibility standards**, ensuring it is usable by people with a wide range of disabilities.

Where a user is unable to access or use the web portal, **alternative access channels** are available. These include:

- Assisted support via email or telephone
- Administrative actions performed on the user's behalf by authorised support personnel

These alternative channels ensure that all users can access the service and receive support regardless of accessibility needs.



Incident Management

This section outlines the SysGroup Operations Team and the process for reporting all faults on any part of your service.

Operations Team Introduction

The SysGroup Operations Team is responsible for the support of your BaaS service and all service issues. The following paragraphs detail the responsibilities and procedures to be followed.

The SysGroup Operations Team is located at:

TBC

Telephone: 0333 101 9000 (option 2)

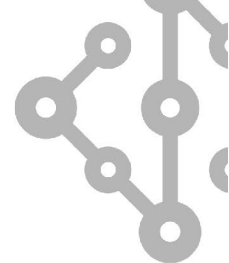
The SysGroup Operations Team is staffed 24 hours a day, 7 days a week and delivers the following functions:

- Receives, logs and progresses incidents
- Investigates and diagnoses technical problems
- Co-ordinates incident resolution with the vendor
- Provides regular progress reports throughout the life of the fault

In addition to these core responsibilities, customers can access SysGroup support through both telephone and email channels. Managed access to the Rubrik Security Cloud is provided via a secure browser interface, where reporting, dashboards and restore operations are available. All interactions related to support, incident management and service requests are handled through SysGroup's ticketing process to ensure full traceability and consistent service delivery.

Personal Security Controls

All members of the SysGroup Operations Team working on CUSTOMER systems shall be vetted to BS7858 standard, ensuring a trusted and secure operational environment. The BaaS platform incorporates a comprehensive set of security measures, including immutable and air-gapped backups underpinned by a Zero Trust Architecture. Data and metadata are fully encrypted, and the service includes ransomware detection, anomaly detection, threat hunting and malware containment to protect against evolving cyber threats. Sensitive data monitoring further enhances the organisation's ability to identify and manage data-exposure risks. All customer data is hosted within the UK to maintain sovereignty, supported by full action logging and audit trails to meet compliance and governance requirements. In addition to platform-level protections, SysGroup maintains strict personnel-security controls, with all Operations staff vetted to BS7858.



Incident Reporting

In the event that the <CUSTOMER> has to report a Priority 1 or Priority 2 fault, they should telephone the SysGroup Operations Team on 0333 101 9000 (option 2). Failure to report the fault via the correct channel will mean that the call is not tracked and monitored in accordance with the SLA and could result in a delay. Priority 3 or Priority 4 requests can be made by email to support@SysGroup.com.

To enable the fault to be logged accurately, persons reporting faults should provide the following information:

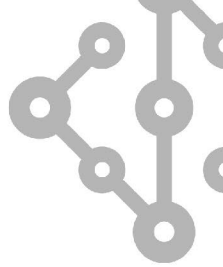
- Company Name
- Contact Name
- Contact Number
- Fault Details

Fault references will be exchanged between SysGroup and <CUSTOMER> at the time of fault reporting. The fault reference number allocated by SysGroup should be used in any subsequent discussion or correspondence regarding the fault report. All faults will be managed within our call management system.

The call will be passed on to an available engineer who will acknowledge receipt of the call and request further diagnostic information if required. Please note that you may be asked to perform troubleshooting on the system and/or supply system files for analysis. Should <CUSTOMER> be unable to provide troubleshooting information for longer than 5 working days, the call will be placed on hold and reactivated when <CUSTOMER> is ready. We have a secure email facility for transmitting and receiving sensitive information such as log files to and from clients. In addition, a wide range of data types including virtual machines, file data, application data, Microsoft 365 data and more can be uploaded to and protected by the BaaS platform.

The SysGroup Operations Team undertakes initial fault diagnosis, and, after analysis, the fault may be passed to other groups within SysGroup or the vendor for repair. However, the SysGroup Operations Team shall retain overall responsibility for the progression and clearance of the fault, providing regular updates on the progress of the repair. <CUSTOMER> user may contact the SysGroup Operations Team at any time to enquire on progress of the fault.

In support of this model, the service also provides telephone and email access to the 24/7 Operations Team, with Priority 1 and Priority 2 issues handled via phone and Priority 3 and Priority 4 issues managed by email. Quarterly service review meetings may be conducted remotely or onsite, and proactive notifications are issued to alert <CUSTOMER> to any relevant updates or issues affecting the service. Quarterly recovery test reports are also provided for customer verification. A wide range of data types—such as virtual machines, file data, application data, Microsoft 365 data and more—can be uploaded to and protected by the BaaS platform.



Escalation Path

In the event of a Priority 1 (i.e. 'Business Down') situation the Service Desk should be the initial point of contact.

If a response time or expectation is not being delivered, then the escalation path should be followed.

This process allows the SysGroup Service Desk to escalate issues of this nature following a strict action-plan should any such business affecting situations occur.

SysGroup

Initial contact to be logged via Service Desk

0333 101 9000 (option2) for all P1 issues

help@sysgroup.com

First Point of escalation

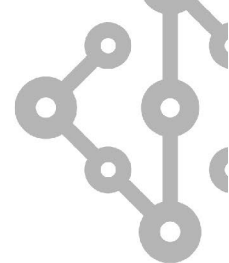
Chris Kaye
Service Desk Manager

Second Point of escalation

Ryan Parker
Service Delivery Manager

Final Point of escalation

Kevin Johnson
Platform Lead – Data Protection



Service Constraints

This Rubrik-based Backup as a Service (Baas) solution has the following constraints.

Connectivity and Network

To use this service, we recommend that customers must have a reliable internet connection with a minimum bandwidth of 10 Mbps per protected workload, although this may vary depending on data volumes and how frequently data changes.

Outbound HTTPS (TCP port 443) access is required for management traffic, and additional network ports may be needed depending on the type of workload being protected. Customers are responsible for ensuring their network has sufficient capacity to support backup and restore operations.

Supported Platforms and Operating Systems

The service supports platforms and operating systems that are supported by Rubrik. This includes VMware vSphere and Microsoft Hyper-V, as well as supported versions of Windows Server and Rubrik-supported Linux distributions such as RHEL, CentOS, Ubuntu, and SUSE Linux Enterprise Server (SLES).

Only platforms and operating systems that are within both vendor and Rubrik support lifecycles are supported.

Application Support

Application-aware protection is available where supported by Rubrik, including for Microsoft SQL Server, Exchange, Active Directory, file systems, and supported NAS platforms. Application consistency and recovery depend on correct configuration and appropriate permissions being in place.

Access Requirements

The management interface is accessed using a modern web browser, such as Google Chrome, Microsoft Edge, or Mozilla Firefox. End-of-life or unsupported browsers are not supported.

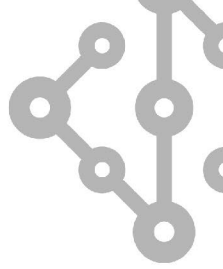
Service Prerequisites and Limitations

Protected workloads must meet Rubrik's minimum requirements for agent-based or agentless protection. Appropriate credentials, permissions, and time synchronisation (for example, using NTP) must be configured.

Backup and restore performance depends on factors such as network conditions, workload performance, and data volumes. The service does not support unsupported or end-of-life platforms or applications. Service availability may be affected during planned maintenance windows, which will be communicated in advance.

Customer Responsibilities

Customers are responsible for maintaining supported workloads and configurations and for meeting their own regulatory, data protection, and retention requirements. Customers are also responsible for validating restores and recovery processes.

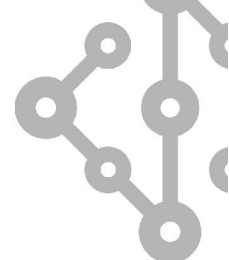


Out of Scope

SysGroup are responsible for the management of all BaaS capabilities procured by <CUSTOMER> and for the remediation of any BaaS-related issues. An example of out-of-scope activities are:

- IDP Management
- Network changes
- FW Rule changes
- Private Key Management
- Policy decisions – CUSTOMER must provide requirements
- End User Computers
- DNS Management
- Host operating system installation or configuration.
- Server and storage hardware installation or configuration.
- Physical cable installation.

Configuring and consuming the service follows a structured process. <CUSTOMER> selects the preferred BaaS tier and architecture, after which SysGroup conducts the onboarding and solution design. Retention policies and backup schedules are then configured in line with agreed requirements. The service is delivered and monitored according to ITIL-based processes, with regular reporting and review activities ensuring continual service improvement.



Service Levels

SysGroup will be working within the service levels defined below. The response time measure begins at the point the call is logged with the SysGroup Level 1 support, and a call reference is assigned and ends when a SysGroup Support Analyst calls CUSTOMER back to discuss the situation. SysGroup BaaS has a 99,9% service availability.

INCIDENT MANAGEMENT SLA's:

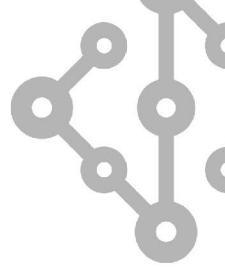
All incident calls will be classified into 4 call severities as shown in the table below.

Call Severity	Description	Response Time
P1 Critical	An issue that prevents operation of critical documented functions with high frequency or duration.	30 mins
P2 Serious	An issue that consistently prevents operation of non-critical documented functions or occasionally impacts critical documented functions or a critical issue for which a temporary work around has been provided.	1 hour
P3 Moderate	An issue that has some impact on administration, non-critical operation or other secondary functions or a major issue for which a temporary work around has been provided.	3 hours
P4 Minor	The BaaS service is unaffected; Customer requests product related technical advice or general information and feature questions related to the Products.	4 hours

SysGroup shall aim to meet these response time levels of service in at least 95% of cases.

How to Buy

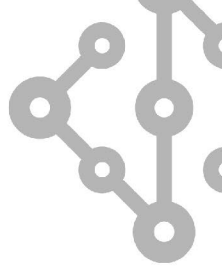
Services are available on annual or multi-year subscriptions, supported by clear service definitions and documented SLAs so the customer understands exactly what is included from the outset. The solution is tailored to the customer's operational and regulatory needs, ensuring the chosen BaaS tier and architecture align effectively with business, compliance and resilience requirements.



CHANGE/SERVICE REQUEST SLA's:

Category	Description	Initial Telephone Response
Standard	<p>SysGroup will initiate 95% of standard service requests per quarter within 8 working hours (Monday to Friday, 08:00 -18:00)</p> <p>Target request completion time is 8 hours.</p>	<p>A Standard request is any pre-authorized activity that is low risk, relatively common and follows a predefined procedure or work instruction. SysGroup's Change Advisory Board (CAB) is not required to approve Standard service requests prior to implementation.</p> <p>All such requests are subject to CUSTOMER'S Change Management Procedure.</p>
Normal	<p>SysGroup will respond to 95% of normal service requests per quarter within 8 working hours (Monday to Friday, 08:00 -18:00)</p> <p>Target request completion time is 8 hours.</p>	<p>A Normal service request is any request that is not a Standard request according to the above definition and is not an emergency. It is an agreed ad-hoc request to modify the configuration of the services. The SysGroup CAB must authorise Normal changes and approve an implementation plan.</p> <p>All such requests are subject to CUSTOMER'S Change Management Procedure</p>
Emergency	<p>SysGroup will initiate 99.5% of required emergency service requests per quarter within 4 hours.</p> <p>Target request completion time is 4 hours.</p>	<p>An Emergency service request is any Normal request that requires an expedited timeframe to resolve an issue that cannot wait for review and approval from the CAB. Usually, a request by the Customer to SysGroup to modify the configuration of the services in response to a PI incident. SysGroup's Emergency Change Advisory Board must authorise Emergency changes and approve an implementation plan.</p> <p>All such requests are subject to CUSTOMER'S Change Management Procedure.</p>

For service requests SysGroup will work with CUSTOMER on a template that ensures all relevant information is captured when raising a service request. The service offers a high degree of flexibility, allowing customers to configure custom retention policies, select the most appropriate architecture and apply tailored security settings, including sensitive data scanning. Backup schedules, protected workloads and data sources can



be adjusted as operational requirements evolve, with full support for Standard, Normal and Emergency change requests. Quarterly service reviews are used to refine, optimise or expand the service, ensuring it continues to align with business priorities and regulatory requirements.

Service Review Meetings

SysGroup will contact CUSTOMER on a quarterly basis to review the service. This will either be conducted over a Teams meeting or via an on-site meeting as deemed appropriate.

Call Frequency

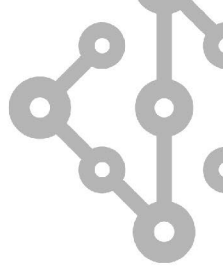
SysGroup reasonably anticipates handling no more than 10 support calls per month and believes that if the call frequency is greater than this, it would signify that CUSTOMER has underlying issues with its Baas service. In this case, SysGroup would expect to discuss the matter at a service review meeting.

Complaints Procedure

If at any time, CUSTOMER feels that their service from SysGroup is unsatisfactory, and that the specific escalation processes outlined in this document have been unable to rectify the situation, CUSTOMER can register a formal complaint. All complaints should be outlined in writing to the SysGroup Quality Manager, Paul Sullivan:

complaints@SysGroup.com

All formal complaints will be acknowledged within 24 hours, and a formal response should be received within 10 working days of receipt. CUSTOMER may give notice during the contracted period; however, they will be required to pay the remainder of the monthly or annual billing for the duration of the agreed contract term.



Change Management

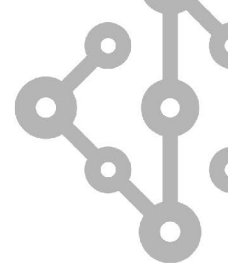
Change Control Notification

It is strongly recommended that <CUSTOMER> advises SysGroup Operations Team of any major changes that they wish to make to the method of integrating the BaaS service. Notifications should be sent to support@SysGroup.com with a subject header of Change Request.

SysGroup will review the change and provide advice on any potential issue with the change. If necessary, SysGroup will update its configuration records for <CUSTOMER> for support purposes. Failure to do so may result in a delay to the resolution of a support call.

It is also strongly recommended that <CUSTOMER> advises SysGroup Operations Team if any other infrastructure changes are occurring that may impact the delivery of BaaS service. The SysGroup Operations team will inform the on-call engineer of the details of the change.

In the event that <CUSTOMER> would like SysGroup to provide telephone or on-site support for the duration of a change, they should contact the SysGroup Operations Manager listed in Appendix A as this may incur a cost to the customer.



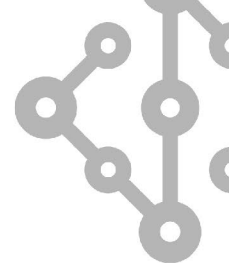
Appendix A – Contact Information

SysGroup Contacts

Name/Title	Telephone	Email
SysGroup Operations	0845 052 2955	support@sysgroup.com
Kevin Johnson	0845 052 2955	kevin.johnson@sysgroup.com

<Customer> Contacts

Name/Title	Telephone	Email



Approved Service Callers from CUSTOMER

Only the following people within CUSTOMER shall be permitted to log support calls with the SysGroup Support Desk:

Name/Title	Telephone	Email
Any CUSTOMER Employee*	-	-