

CyberArk Managed Operations Service

Privilege Cloud Service Description Document

SysGroup

Contents

1. Distribution and Revision 4
1.1. DOCUMENT DISTRIBUTION LIST 4
2. Introduction 5
2.1. OPERATIONS 5
2.2. PRO-ACTIVE APPROACH 5
2.3. DOCUMENTATION 5
2.4. UNIQUE SERVICE BENEFITS 5
2.5. ACCESSIBILITY STANDARDS 6
3. Onboarding & Offboarding Process 7
3.1. SERVICE ONBOARDING 7
3.2. SERVICE OFFBOARDING 7
3.2. SERVICE OFFBOARDING 8
4. Definitions and Sign-Off 8
4.1. PARTIES & DEFINITIONS 8
4.2. REVISIONS TO THE DOCUMENT 8
4.3. SYSGROUP SIGN-OFF 9
4.4. CUSTOMER SIGN-OFF 9
4.5. CONTRACT PERIOD 9
5. Managed Operations 10
5.1. Introduction 10
5.2. SERVICE OPERATING HOURS 10
5.3. OPERATIONS TEAM INTRODUCTION 11
5.4. System Health 12

5.5. System Management 13
5.6. System Reporting 14
5.7. Cyberark Account Management 14
5.8. Customer Requirements 15
5.9. Out of Scope 16
5.9. Service Levels for Service Requests 17
5.11. Service Levels for Change Requests 18
5.12. Incident Reporting 19
5.13. Service Levels for Incident Response 20
5.14. Service Credits 21
5.15. Customer Site Access 22
5.16. Service Review Meetings 22
5.17. ESCALATION PROCESS 22
5.18. Complaints Procedure 23
6. Maintenance and Support 24
6.1. Renewal Policy 24
6.2. Cyberark License Management 24
6.3. Cyberark System Upgrades 24
6.4. Patching 25
7. Technical Advice and Consultancy 26
7.1. Requesting Technical/Product Advice 26
Appendix A - Contact Information 27
Appendix B - CyberArk Maintenance Certificate 28
Appendix C - Remote Access Method Description 29

1. Distribution and Revision

1.1. DOCUMENT DISTRIBUTION LIST

Version Control

Name	Company	Email Address

2. Introduction

The purpose of this document is to provide the customer with a definition of the CyberArk Managed Operations Service delivered by SysGroup. It states the expected service levels, the available recourse if they are not met, and is subject to the Master Services Agreement in operation between CUSTOMER and SysGroup. CUSTOMER owns and operates all CyberArk systems to OS level. SysGroup is responsible for delivering all operational activities to support, maintain, and operate the CyberArk systems including all CyberArk software upgrades and SysGroup own the CyberArk licenses.

The document defines the agreed procedures to be followed for all operational procedures to support the CyberArk solution. It provides a general description of service scope, the service request processes, and information on roles and responsibilities.

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 CUSTOMER will receive high-quality Incident, Problem and Change Management, managed centrally by our fully trained and dedicated Operations team.

2.1. OPERATIONS

The SysGroup Operations Team is responsible for supporting your CyberArk solution. The Operations Team will log and progress service requests, faults and technical queries. They will issue you with a reference number and keep you informed on the progress of your request. The Operations Team will operate within the agreed service levels for incident response, service requests and change requests.

2.2. 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 CyberArk upgrade with functionality relevant to CUSTOMER, is available. Similarly, if SysGroup is made aware of any CyberArk issues via their Security Bulletin channel that are relevant to CUSTOMER, we will notify you to agree the next steps.

2.3. DOCUMENTATION

SysGroup will ensure that all documentation relating to the managed service is maintained, valid and can be provided in a timely way to CUSTOMER upon request.

2.4. UNIQUE SERVICE BENEFITS

In addition to the core managed support activities described above, SysGroup provides several service features that offer clear advantages compared to alternative support offerings in the digital marketplace.

These benefits include:

- Operation by a 24/7 UK-based Operations Team with strong CyberArk expertise and ITIL-aligned service management processes
- Direct coordination with CyberArk vendor support on behalf of the customer to speed up investigation and resolution of complex issues
- Proactive monitoring of CyberArk updates, issue advisories and functional changes, ensuring the customer is informed of any developments that may affect their environment
- Clearly defined SLAs, response targets and escalation routes to ensure predictable and accountable service delivery
- Accelerated diagnostics enabled through delegated access to the customer's CyberArk administration interface, supported by optional test-user creation where needed
- A purpose-built managed service specifically focused on supporting CyberArk cloud security, rather than a general network or IT support model

These elements together provide a managed service with enhanced responsiveness, deeper technical insight and stronger operational oversight than typical marketplace alternatives.

2.5. ACCESSIBILITY STANDARDS

SysGroup confirms that customer-facing service channels, documentation and digital interfaces under its control are designed to align with WCAG 2.1 Level AA accessibility standards, where applicable. This includes consideration for:

- Visual, auditory, motor and cognitive accessibility needs
- Clear, readable communications and documentation
- Compatibility with commonly used assistive technologies

3. Onboarding & Offboarding Process

3.1. SERVICE ONBOARDING

Service onboarding is initiated following contract signature and confirmation of CyberArk license procurement. The onboarding process is designed to ensure secure, controlled access and a smooth transition into steady-state managed service operations.

Onboarding activities include:

- Formal service initiation request agreed between the customer and SysGroup
- Provisioning of role-based access for authorised SysGroup engineers to the customer's CyberArk Administration Interface
- Validation of access controls, audit logging and least-privilege permissions
- Configuration of service contacts, escalation paths and approved service callers
- Optional creation of a customer-controlled test user within the customer's Identity Provider (IDP) to support diagnostics and troubleshooting
- Verification of incident reporting, change management and communication processes
- Confirmation that monitoring, operational records and support tooling are correctly configured

On completion of onboarding, the service transitions into business-as-usual operations and is governed by the SLAs, escalation procedures and service review cadence defined within this document.

3.2. SERVICE OFFBOARDING

Service offboarding may occur at contract expiry, termination or by mutual agreement. Offboarding is managed in a structured and auditable manner to ensure security, continuity and data protection.

Offboarding activities include:

- Formal notification of service termination and agreement of an offboarding plan
- Removal or revocation of all SysGroup access to the customer's CyberArk Administration Interface
- Decommissioning of any SysGroup-managed service accounts or credentials
- Secure handling and disposal of customer data in line with contractual and regulatory obligations
- Final service reporting if requested
- Support for transition to an alternative provider where agreed

Unless otherwise agreed, offboarding activities are completed within agreed exit SLAs, and SysGroup will provide reasonable cooperation to ensure an orderly and secure service transition.

3.2. SERVICE OFFBOARDING

Service offboarding may occur at contract expiry, termination or by mutual agreement. Offboarding is managed in a structured and auditable manner to ensure security, continuity and data protection.

Offboarding activities include:

- Formal notification of service termination and agreement of an offboarding plan
- Removal or revocation of all SysGroup access to the customer's CyberArk Administration Interface
- Decommissioning of any SysGroup-managed service accounts or credentials
- Secure handling and disposal of customer data in line with contractual and regulatory obligations
- Final service reporting if requested
- Support for transition to an alternative provider where agreed

Unless otherwise agreed, offboarding activities are completed within agreed exit SLAs, and SysGroup will provide reasonable cooperation to ensure an orderly and secure service transition.

4. Definitions and Sign-Off

4.1. PARTIES & DEFINITIONS

This document has been agreed between the following parties:

(1) SysGroup PLC, is a company registered in England No. 06172239. Registered office is at Walker House, Exchange Flags, Liverpool, L2 3YL, hereby referred to throughout this document as "SysGroup"

and

(2) Customer

4.2. REVISIONS TO THE DOCUMENT

SysGroup will release a revised handbook upon renewal of the CyberArk support & maintenance contract to reflect the updated certificate as shown in Appendix B.

SysGroup will also release a revised handbook should CUSTOMER inform them of any changes to the table shown in Appendix A. Changes to the Appendixes will not require formal sign-off from either party. However, should SysGroup release a revised handbook following any changes to section 3 to 7, sign-off will be sought from CUSTOMER and SysGroup.

4.3. 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:

Name: Bryan Thomson

Position: Director of Cyber

Signature:

4.4. CUSTOMER SIGN-OFF

Upon sign-off of this document, CUSTOMER commits to following the processes outlined in sections 3 to 7 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:

4.5. CONTRACT PERIOD

The period of support for this service is from <CONTRACT TERM DATES>

5. Managed Operations

5.1. Introduction

SysGroup's CyberArk Managed Operations Service will operate and manage your CyberArk systems to ensure you get the most out of your investment. Our highly adept security engineers work together with you to provide product consultation, including answering questions, building product knowledge and advising you on system recommendations. Further to this we will also take care of the day-to-day tasks involved with the management of your CyberArk platform.

CyberArk provides enterprise grade Privileged Access Management delivered as a fully managed, turnkey service designed for specifically for UK organisations and regulated environments. CyberArk has several unique selling points including:

- Deep CyberArk expertise built over more than seven years, with multiple technical and sales certifications.
- Strong endorsement from CyberArk leadership for high-quality delivery, deep technical understanding and ongoing customer success.
- Proven track record delivering managed services for banking, insurance, and public sector organisations.
- Fully managed 24/7/365 operations including monitoring, patching, upgrades, fault resolution and reporting.
- Designed to meet UK compliance, governance, audit and operational resilience expectations.

This section of the document will explain in detail the parameters of the SysGroup Managed CyberArk service.

5.2. SERVICE OPERATING HOURS

5.2.1. Hours of Operation

Standard Business hours, Monday to Friday; 08:00 - 18:00

5.2.2. Out-of-Hours

Monday to Friday 18:00 to 08:00, and Friday 18:00 to 08:00 Monday

5.3. OPERATIONS TEAM INTRODUCTION

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

SysGroup can offer a number of deployments for the operations team including

- On-premise CyberArk deployments.
- Hybrid deployments.
- Migrations between on-premise and cloud CyberArk platforms.

These deployments are delivered through professional services or hybrid managed models depending on customer requirements.

In addition, the core services are delivered online as a managed cloud service using CyberArk Privilege Cloud. Customers access the service securely via the internet using browser access, APIs, and secure session tools.

The SysGroup Operations Team is located at:

SysGroup

Sugar Bond

2 Anderson Place

Edinburgh

EH6 5NP

Telephone: 0333 101 9000

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

- Receives, logs and progresses service requests.
- Investigates and diagnoses technical issues.
- Co-ordinates issue resolution with CyberArk as required.
- Provides regular progress reports throughout the life of a service request.

Our service delivers the following benefits:

Security benefits:

- Centralised storage of all privileged credentials in an encrypted vault.
- Automated password rotation, removing static credentials.
- Zero standing privilege model with access granted only when required.
- Full session isolation, monitoring and recording.
- Continuous 24/7 monitoring, threat analytics and system health oversight.

Operational benefits:

- Removes the need for in-house PAM specialists.
- Reduces operational overhead such as patching, upgrades and daily administration.
- Faster implementation and ongoing optimisation.
- Clear service levels for incidents, changes and service requests.

Compliance benefits:

- Complete audit trails of privileged activity.
- Enables demonstration of accountability and access governance.
- Supports UK GDPR, public-sector audit, and operational resilience expectations.

Scalability and futureproofing:

- Always kept current with the latest CyberArk capabilities.
- Supports cloud, on-premises and hybrid environments.

5.3.1. Personnel Security Controls

All members of the SysGroup Operations Team working on CUSTOMER systems shall be vetted.

5.4. System Health

SysGroup will continually monitor the health of your CyberArk systems in a 24 x 7 capacity. Specific tasks include:

- 24x7 CyberArk platform continuous monitoring to ensure system availability for the following components:
  - Privilege Cloud Connectors (PSM, CPM, Secure Tunnel Client)
  - Unix Connector (PSM for SSH)
  - Credential Providers if any
- Central Password Manager (CPM) Issue Resolution
  - CyberArk CPM Failure for Scheduled Tasks
  - CyberArk CPM Failure for Verify Only Accounts
  - CyberArk CPM Failure for Fully Managed Accounts

5.5. System Management

SysGroup will conduct the following tasks as part of the System Management function on your CyberArk platform:

Category	Task Description
Safe Management	• Add Safes • Update Safe Properties • Manage Safes – rename and delete safes. • Add Safe Members • Add Safe Members from LDAP • Remove Safe Members • Update Safe members authorisations
Component Management	• Component Configuration Changes • System Configurations Changes • Recreate User Credential Files • Component Log Management
Platform Management	• Create, Modify & Delete Platforms used for automatic managements of Accounts. • Manage Master policy rules and settings. • Apply Platforms to safes. • Verify, Reconcile passwords. • Associate Logon Accounts. • Import Packages • Update the Master Policy Rules & Exceptions
Patching	• Connector Patching
Minor Changes	• Add additional SMTP servers

5.6. System Reporting

SysGroup will generate and manage reports regarding your CyberArk platform on a regular basis. Details of these reports are as follows:

Category	Task Description
Reports	• Weekly Compliance Reports • Monthly CPM Reporting • Monthly Component Health Check

5.7. Cyberark Account Management

As part of the service SysGroup will manage all account activity on your CyberArk system. We expect that the majority of user management will be done by the client provisioning team, however, we do expect to work in conjunction with them to perform some meta-tasks; for example, the bulk onboarding of accounts using a restapi script.

Category	Task Description
Account Management	• CyberArk Add and Delete Accounts • Manage Service Account Passwords • Management Processes for Personal Admin Accounts within CyberArk • Manual Password Change Process • Scan for Accounts using Accounts Discovery • Manage privileged sessions • Support of manual change password process when password synchronisation is lost and no reconciliation account exists. • Six-Monthly Review of CyberArk Access and Personal Admin Accounts within CyberArk • Provision of enhancement and feature requests to CyberArk
User Management Enablement	• Identity Directory Mapping • Templates and permission management
Managed Service Governance	• Service would operate to defined response time SLA's and within a service credit regime

5.8. Customer Requirements

To allow SysGroup to deliver our Managed CyberArk service to our CUSTOMER the following requirements must be agreed upon:

Requirement	Description
User Management	User management is operated by the client provisioning team. SysGroup will not have any access to the clients IDP which is typically Active Directory
Remote Access	SysGroup requires full remote access to all of the CyberArk systems within the scope of management. For example, providing SysGroup with a suitable asset provided and maintained by the CUSTOMER (such as a laptop), or access via the Corporate remote access solution from a third-party device
Custom Reporting	The number of requests for the creation of custom reports is limited to six per quarter. Any additional requests shall be scoped and delivered on a professional services basis
Approved Callers	The client will define a list of approved callers, and all approved callers must have a basic appreciation CyberArk technology
Maintenance Contract	Clients must have a valid maintenance contract with CyberArk that covers the duration of the SysGroup Managed Service

During implementation Sysgroup uses a structured four phase approach.

Phase 1 – Discovery and Planning:

- Privileged account inventory.
- Risk assessment.
- Policy design.
- Identity provider and MFA integration planning.

Phase 2 – Build and Configuration:

- Tenant provisioning.
- Safe structure and permissions.
- Onboarding of systems such as Windows, Linux, databases and cloud.
- Password policies.
- Session isolation configuration.

Phase 3 – Testing and User Acceptance:

- Workflow testing.
- Pilot validation.
- Security control checks.
- Resilience and disaster recovery testing.

Phase 4 – Training and Go-Live:

- Administrator and user training.
- Go-live support and hyper care.
- Transition to business-as-usual managed service.
- Consumption:
- Browser access to the CyberArk Privilege Cloud interface.
- Use of secure session tools for RDP and SSH.
- Automation or API calls for onboarding accounts.
- Receiving scheduled reporting from SysGroup.
- Raising service requests, incidents and changes via the support process.

5.9. Out of Scope

The following activities are out-of-scope of the SysGroup Managed CyberArk service:

Task	Description
CyberArk Plug-in development	Create custom CPM plug-ins and the universal connection component (PSM)
Major changes to the CyberArk infrastructure	Installing additional components & changes to the architecture

SysGroup can perform activities which are out-of-scope of the Managed Service discrete professional services engagements. Where initiated by the CUSTOMER, the CUSTOMER can formally request a major change to the CyberArk infrastructure with the nominated SysGroup Account Manager who will acknowledge, review and respond in a mutually agreed timescale.

5.9. Service Levels for Service Requests

SysGroup will be working within the managed operations service levels defined below. All service requests will be classified into three categories as shown in the table below:

Service Request Category	SLA	Definition
Standard	SysGroup will initiate 95% of standard service requests per quarter within 8 working hours (Monday to Friday, 08:00 - 18:00) Target request completion time is 8 hours.	A Standard request is any pre-authorised 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. All such requests are subject to CUSTOMER'S Change Management Procedure.
Normal	SysGroup will respond to 95% of normal service requests per quarter within 8 working hours (Monday to Friday, 08:00 - 18:00) is 8 hours.	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. All such requests are subject to CUSTOMER'S Change Management Procedure.
Emergency	SysGroup will initiate 99.5% of required emergency service requests per quarter within 4 hours. Target request completion time is 4 hours.	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 P1 incident. SysGroup's Emergency Change Advisory Board must authorise Emergency changes and approve an implementation plan. All such requests are subject to CUSTOMER'S Change Management Procedure.

5.11. Service Levels for Change Requests

SysGroup will be working within the managed operations service levels defined below. All change requests will be classified into three categories as shown in the table below:

Change Request Category	SLA	Definition
Standard	SysGroup will initiate 95% of standard change requests per quarter within 8 working hours (Monday to Friday, 08:00 - 18:00) . Target request completion time is 8 hours.	A Standard change request is any pre-authorised change 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 change requests prior to implementation. All such requests are subject to CUSTOMER'S Change Management Procedure.
Normal	SysGroup will respond to 95% of normal change requests per quarter within 8 working hours (Monday to Friday, 08:00 - 18:00). Target request completion time is 8 hours.	A Normal change 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 change the configuration of the services. The SysGroup CAB must authorise Normal changes and approve an implementation plan. All such requests are subject to CUSTOMER'S Change Management Procedure.
Emergency	SysGroup will initiate 99.5% of required emergency change requests per quarter within 4 hours. Target request completion time is 4 hours.	An Emergency change 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 change the configuration of the services in response to a P1 incident. SysGroup's Emergency Change Advisory Board must authorise Emergency changes and approve an implementation plan. All such requests are subject to CUSTOMER'S Change Management Procedure.

5.12. Incident Reporting

SysGroup will identify most CyberArk system issues before CUSTOMER is aware of them. However, in the event that CUSTOMER has to report an incident, they should alert the SysGroup Operations Team (Section 5.1) by a call, email or via the portal (contact details below). The Managed Operations Service operates on a 24x7 basis so incidents can be logged at any time. Failure to report the incident via the correct channel will mean that the call is not tracked and monitored in accordance to the SLA, and could result in a delay.

Phone: **+44 (0) 333 101 9000**

Email: **cybersupport@sysgroup.com**

Portal: **support.sysgroup.com**

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

- Company Name
- Contact Name
- Contact Number
- Product
- Incident Details

Incident references will be exchanged between SysGroup and CUSTOMER at the time of incident reporting. The incident reference number allocated by SysGroup should be used in any subsequent discussion or correspondence regarding the incident report. All incident will be managed within our ticket management system.

The ticket will be passed on to an available engineer who will acknowledge receipt and who may request further (non-CyberArk System) diagnostic information if required. Please note you may be asked to perform troubleshooting on related systems (such as the network) and/or supply system non-CyberArk files for analysis. Should CUSTOMER be unable to provide troubleshooting information for longer than 5 working days, the ticket will be placed on hold and activated when CUSTOMER is ready. SysGroup has a secure email facility for transmitting and receiving sensitive information such as log files to and from clients.

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

When the SysGroup Operations Team has resolved the issue, they will mark the issue as resolved within the system and stop the incident timer.

In order to support the incident reporting process, customers may upload supporting files required for troubleshooting, configuration or analysis.

The acceptable file formats for the different types of files are as follows:

- Log files: txt, log, zip
- Configuration files: xml, json, csv
- Documentation: docx, pdf
- Screenshots: png, jpg

Sysgroup ensures that secure communication methods are used for exchanging sensitive files

5.13. Service Levels for Incident Response

SysGroup will be working within the service levels defined below. The response time measure begins at the point the ticket is created with the SysGroup Level 1 support and a ticket reference is assigned, and ends when a SysGroup Support Analyst calls CUSTOMER back to discuss the situation.

All incidents will be classified into four severities as shown in the table below:

Incident Severity	Description	Initial Telephone Response
Critical	A down situation, whereby a CUSTOMER is unable to do production work, and a workaround is not available. This category includes: • the CyberArk system ceases to be operational • the product requires repeated reboots of the system	1 hour
Serious	A major function is unusable and no workaround is available, but the CUSTOMER is able to do some production work. The Product may: • be usable but incomplete (one or more major documented commands/functions are inoperable/missing) • require rebooting of one or more elements of the system • suffer sufficient degraded performance (throughput/response) such that there is a severe impact on usability.	2 hours
Moderate	There is a loss of a function or resource that does not seriously affect the CUSTOMER's operations or schedules. Any problem, which was originally reported as Critical or Serious, but has been temporarily solved with a workaround, shall be reduced to Moderate.	6 hours
Minor	Means all other problems with the Product(s) other than those falling within the categories above. This category includes: • errors in Product Documentation • instances when the Product does not operate strictly according to specifications	12 hours

SysGroup shall aim to meet these response time levels of service in at least 95% of cases. For critical and serious incidents, SysGroup will assign a dedicated Incident Manager who will be responsible for managing the progress of the incident response and ensuring timely and appropriate communications with CUSTOMER.

5.14. Service Credits

The response times SLAs measure how long it takes SysGroup to respond to service requests, change requests and incidents. SysGroup is deemed to have responded to an incident or a request when a case is created in SysGroup's support system and a ticket number is allocated. SysGroup is deemed to have responded to a normal service or change request when a ticket is created in SysGroup's support system and the change has been allocated to an engineer queue for planning to commence. A Standard or Emergency service or change is initiated at the point at which (as recorded in the support system) SysGroup commences the implementation of the change.

SysGroup will measure its response times over a three-month period (a quarter) and calculate the proportion of incidents responded to, or service requests or change requests initiated, within the target response times. The data will be included in quarterly service delivery reports.

The service review period shall be three months. If in any given quarter, more than 5 incidents or service or change requests have occurred and SysGroup fails to achieve any of the SLAs in respect of response or initiation times, then the CUSTOMER will be eligible for a service credit against the charges for service management as follows:

Service Level Performance Over 3 Months	Service Credit
0 to 10% below target	Meets SLA, no service credit
11% to 25% below target	10% of the quarterly charges
26% to 50% below target	20% of the quarterly charges
51% to 75% below target	50% of the quarterly charges
76% to 100% below target	100% of the quarterly charges

While not subject to the service credit regime, if SysGroup is repeatedly missing target completion times for service and change requests, then CUSTOMER can request an immediate interim service review conference call to discuss the root cause(s) and remedial actions.

5.15. Customer Site Access

In the first instance, all support calls will be investigated and resolved remotely with the assistance of CUSTOMER, if and when required. However, in the unlikely event that, during the progression of a support call, it is identified and agreed by all parties that a SysGroup or vendor engineer requires physical access to the vaults, the following process will be followed:

- All parties agree which site the engineer needs to access
- CUSTOMER will make the access arrangements as per current procedure
- CUSTOMER will provide SysGroup with the incident reference number from their support system for verification purposes
- SysGroup will confirm the name of the engineer being sent to site
- The SysGroup or vendor engineer will arrive at site with the SysGroup support reference, the CUSTOMER fault reference and a form of photographic ID such as driving licence, passport, company ID etc.

Users access the service through secure, controlled channels including web browser access to the CyberArk Privilege Cloud portal, integration via corporate identity providers with MFA, session tools such as CyberArk PSM for RDP and SSH, and APIs for automation and system integrations.

5.16. Service Review Meetings

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

The meetings will include a discussion of SLA reports and open tickets. All discussion points and actions will be minuted. The meetings can be held in person or by conference call at the request of CUSTOMER. CUSTOMER has the flexibility to request bring forward the next meeting. Changes to service scope would be discussed at this forum.

It is expected that the first service review meeting will take place four to six weeks after the service is initiated so that commencement issues can be resolved and the SysGroup and CUSTOMER interfaces can be optimised quickly.

5.17. ESCALATION PROCESS

In the event of an escalated service issue, SysGroup's Operations Manager will own it. Throughout the duration of the issue, they will liaise with both CUSTOMER and CyberArk in order to achieve a resolution. A full service review will be conducted upon resolution. Should CUSTOMER be dissatisfied with the performance of SysGroup or CyberArk, this will be escalated to Paul Sullivan, Director, to discuss with CUSTOMER and agree any appropriate action to be taken.

SysGroup or CUSTOMER may initiate case escalation. If the SysGroup Operations Team is unable to resolve a problem they will escalate to the relevant support groups within SysGroup, or the vendor. This will normally occur as soon as an increase in the level of staff skill or diagnostic aid is required or if, within a reasonable timeframe from receipt of the fault report, no progress on the fault is being made.

CUSTOMER may escalate at any time if the situation warrants; for example, impact of incident or unsatisfactory response from the SysGroup Operations Team.

Level	Role	Contact	Number
1st Level	Cyber Team Lead	James Phillips	+44(0)3331019000
2nd Level	Account Manager	Elliot Mankoo	+44(0)3331019000

Whenever necessary, the Operations Team Manager will actively monitor the progress of the escalated issue, ensuring that all escalation processes are being effectively utilised and that CUSTOMER is kept informed of progress throughout its duration.

Pricing typically consists of a fixed managed service fee scaled to the size and complexity of the privileged estate, alongside CyberArk Privilege Cloud licence subscription costs. Optional professional services may be engaged for major architectural changes, integrations or migrations, and enhanced services such as monthly privileged account scanning or CISO-level deep-dive reviews can also be added. Pricing is transparent, consumption-based and aligned to the number of accounts, components and integrations required.

5.18. Complaints Procedure

If at any time, CUSTOMER NAME 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 NAME can register a formal complaint. All complaints should be outlined in writing to the SysGroup Quality Manager, James Phillips:

complaints@sysgroup.com

All formal complaints will be acknowledged within 24 hours, and a formal response to your complaint should be received within 10 working days of receipt.

6. Maintenance and Support

6.1. Renewal Policy

It is a prerequisite of the SysGroup service that CUSTOMER has a valid CyberArk support agreement that covers the duration of the SysGroup service. This ensures that CUSTOMER has the right-to-use all applicable software updates for the duration of the service.

CyberArk prefers to adopt a forward renewal policy in relation to maintenance and support provision. CUSTOMER will be required to purchase a support agreement for each additional purchase of any CyberArk products or components.

However, at the time of the annual support renewal, CUSTOMER may be asked to make a payment for a longer or shorter amount of time to bring the renewal date in line with the renewal dates of other products and components (a practice known as co-terming). If this applies, CUSTOMER will be contacted by the SysGroup Operations Manager to explain the charges that will be shown on the invoice.

SysGroup will provide CUSTOMER with a quotation approximately 90 days before renewal is required. CUSTOMER will raise a purchase order against the quotation. SysGroup will provide an invoice that CUSTOMER must settle within the agreed terms prior to support expiring.

6.2. Cyberark License Management

SysGroup will manage the CyberArk licenses to ensure that licenses in use are valid and will give advance notification to CUSTOMER where additional licenses will be required.

6.3. Cyberark System Upgrades

The support agreement covers the provision of updated licences and media for major version changes and interim minor releases, along with email and telephone support from SysGroup. SysGroup will discuss the CyberArk upgrade roadmap at quarterly service review meetings and agree a plan of action.

6.3.1. Major Software Upgrade

As part of its Managed Operations Service for CyberArk, SysGroup is expecting to perform one major CyberArk upgrade per year. SysGroup will create a Statement of Work (SoW) that details the tasks associated with the upgrade including planning, pre-production testing, production implementation and testing. The upgrade will commence once CUSTOMER has signed the SoW and allocated the agreed resources to the upgrade activities if any are required.

6.3.2. Minor Software Upgrades

As part of its Managed Operations Service for CyberArk, SysGroup is expecting to perform up to four minor CyberArk upgrades per year. SysGroup will create a Statement of Work (SoW) that will detail the

tasks associated with each minor upgrade including evaluation and planning, pre-production testing, production implementation and testing. The upgrade will commence once CUSTOMER has signed the SoW and allocated the agreed resources to the upgrade activities if any are required.

6.3.3. How to buy

A typical buying process follows a straightforward sequence. The customer begins by identifying privileged access requirements and desired security or governance outcomes. SysGroup is then selected under the appropriate G-Cloud lot, after which a discovery call and scoping session are arranged to confirm requirements. SysGroup provides a Statement of Work and associated pricing, and the customer issues a call-off contract. The discovery and implementation phases then commence. SysGroup supports customers throughout this stage with initial assessments, workshops and planning documentation, ensuring a clear and structured route into service adoption.

6.3.4. Leaving the service

SysGroup has a structured off-boarding process designed to ensure a smooth transition and prevent any disruption to operational environments. As part of this process, SysGroup will export all relevant audit logs, configuration data and session evidence, and will return all customer-owned data in accordance with agreed requirements. Privileged accounts and access pathways created or managed during the service will be fully decommissioned, and SysGroup can provide assistance with migration to another provider or an internal team where needed. Confirmation of data deletion will be provided where required, ensuring a secure and compliant exit from the service.

6.3.5. Other Services

SysGroup offers a range of additional services to enhance privileged access management and broader security operations. These include monthly privileged account discovery scanning to maintain visibility of high-risk identities, as well as CISO-level advisory reports and executive dashboards that provide strategic oversight of security posture. SysGroup can also deliver migration packages to support customers transitioning from on-premise deployments to CyberArk Cloud, along with advanced integrations across SIEM, ITSM and identity platforms. For organisations seeking wider security support, SysGroup provides comprehensive security assessments and managed security operations to strengthen resilience across the entire environment.

6.4. Patching

6.4.1. CyberArk Component Patching

CUSTOMER will be responsible for the OS patching on all CyberArk component servers with the exception of the CyberArk vault servers.

The CPM, PVWA & PSM (connector) virtual servers will be patched following CUSTOMERs Tier and Wave patching cycles.

6.4.2. Vault Server Patching

The vault and PVWA infrastructure is fully managed and patched by CyberArk as part of the Privilege Cloud service. Please refer to CyberArk's terms and conditions for the privilege cloud service. - https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-cloud-security-datasheet

7. Technical Advice and Consultancy

This section outlines how CUSTOMER should contact SysGroup for technical advice that does not constitute a service request.

7.1. Requesting Technical/Product Advice

CUSTOMER should send an email to cybersupport@sysgroup.co.uk with a subject header of Technical Enquiry when you require technical or product advice that is not related to a service affecting issue.

SysGroup will log the service request in the call management system and assign it to an available consultant. The consultant will acknowledge receipt of the request within 24 hours. The time it will take to answer the request fully will depend on the complexity of the enquiry.

Appendix A - Contact Information

SysGroup Contacts

Name/Title	Telephone	Email

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

Appendix B - CyberArk Maintenance Certificate

Appendix C - Remote Access Method Description

Copyright

The content of these pages, unless otherwise stated, is the property of SysGroup PLC and as such is copyright protected. All rights reserved. Material may not be copied, republished or redistributed, in full or in part, for commercial purposes or gain.

SysGroup PLC

+44 (0) 333 101 9000

cybersupport@sysgroup.com

www.sysgroup.com