



Redcentric Partner Cloud Service Definition

April 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1	Service Overview	4
1.1	Service Description	4
1.2	Key Features	5
1.3	Key benefits	5
1.4	Evergreen Host Options	5
1.5	Locations	6
1.6	How users work with the service	6
1.7	Virtual Machine Specification	6
1.8	Virtual Machine Operating System	6
1.9	Over Subscription	6
1.10	Storage	6
1.11	Storage Performance	7
1.12	Encryption at Rest	7
1.13	Network access	8
2	RACI Matrix	9
2.1	Platform RACI	9
2.2	Virtual Resource RACI	10
2.3	Out of Scope Services	11
3	Software Licensing	11
3.1	Licensing usage reporting	11
3.2	Software Licensing Compliance	11
4	Onboarding and Offboarding	11
4.1	Getting started	11
4.2	Offboarding	12
4.2.1	End of contract data extraction	12
4.2.2	End of contract additional assistance	12
4.2.3	Resource Deletion	12
5	Service Levels and Service Credits	13
5.1	Incident Priority Definitions	13
5.2	Incident Response and Resolution Targets	13
6	Guaranteed availability	14
7	Lifecycle Management and Maintenance	14
8	Restrictions, Rights, Obligations, and Terms	15
8.1	Backups & Disaster Recovery	17
8.2	Updates	17
8.3	Discovery Burden	17
8.4	Amendments	17
8.5	Definitions & Interpretation	17

9	Service management	18
	Appendix 1 – Data Processing Statement	20
	Scope 1 – Processing related to the Services	20
	Scope 2 – Processing related to the management of the contract.....	22

1 Service Overview

This service definition applies to customers of Redcentric's Partner Cloud service and supplements the associated SoW and MSA. Redcentric Partner Cloud is a Redcentric provided Infrastructure as a Service (IaaS) offering built on VMware Cloud Foundation that enables partners and their customers to consume compute, storage, and network infrastructure through a simple unified platform.

Redcentric provides two models for this service.

The Adopt service allows a customer to realise their investment in existing infrastructure, provided that the adopted infrastructure is compatible with supported versions of VMware Cloud Foundation (VCF).

The Evergreen service adds HCI infrastructure, delivered and supported by Redcentric in a Opex model. Redcentric will maintain compatibility with supported versions of VCF for the full term of the Evergreen contract.

Core product features for Redcentric Partner Cloud include and are limited to:

- Flexible scale out capabilities
- Self-service portal
- Rack-mounted servers
- Top or rack switches for hand-off to customer network
- Network switches and firewalls for remote access
- Service resilience based on N+1 industry best practice
- VMware Cloud Foundation Licensing

The service uses a co-management model where the customer is responsible for everything above the VCF level unless specified in the associated Statement of Work (SoW). The service will be delivered at the location(s) confirmed in the SoW.

1.1 Service Description

Using an infrastructure licensed and supported by Redcentric customers are able to:

- Provision, modify or delete virtual compute resources
- Provision, modify or delete virtual storage resources
- Provision, modify or delete virtual network resources
- Upload, create and manage virtual machine templates
- Add, modify, or remove segregated VPC internal networks
- Modify the resource configurations for their virtual resources
- Power virtual machines on and off
- Access the virtual console of the virtual machine
- Manage virtual machine snapshots
- Deploy and manage virtual machine backups
- Deploy and manage virtual machine disaster recovery using 3rd party technologies which are supplied by the customer
- Deploy and manage virtual machine disaster recovery using VCF Add-on technologies subscribed to as part of the provided service
- Add or delete users via integrated user directory service.

1.2 Key Features

- Hosted in customer premises
- Self-service portal
- Flexible CPU, Memory, and disk configurations
- Support for multiple access methods to VMs
- Service resilience based on N+1 industry best practice
- Automatic VM placement across host clusters to ensure optimal performance
- Support escalations to Broadcom

1.3 Key benefits

Protect your existing investment – leverage your pre-existing data centre investments

High Availability – Resilient design to keep business critical applications.

Seamless customer experience – Support your customers as you do today, offer a richer experience tomorrow by leveraging enhanced platform features.

Aligned to your needs – Use your existing virtual estate or choose the infrastructure you consume from us.

Aligned to your customers' needs – Define virtual resources in any supported configuration, no limits on fixed sizes to optimise costs.

Secure - Enjoy peace of mind through Redcentric's Cyber Essentials Plus certification and Government vetted engineers.

Focus on customer value – Release time for customer focused initiatives through a fully managed Infrastructure as a Service that takes care of the infrastructure

1.4 Evergreen Host Options

The following table details the specification of host servers that a customer can subscribe to. The exact spec is subject to change as hardware supply from OEMs demand. Additional size options may be added as Redcentric continue to develop the service options. All hosts in a cluster must be a consistent specification.

Size	CPU Architecture	Cores	RAM	Raw NVME Capacity
Small	AMD	32	768 GB	32 TiB
Large	AMD	64	1536 GB	64 TiB

Redcentric will supply additional capacity increments by scaling out the cluster with a consistent and supported architecture.

Customers are responsible for demand forecasting and timely contract amendment signature to ensure that any additional capacity can be provisioned in advance of need.

1.5 Locations

The service can be deployed in any data centre that meets the environmental specifications.

1.6 How users work with the service

Redcentric provides self-service portals that the customer can use to create, edit, manage and delete virtual machines and networks within their virtual datacentres. The customer can

- Provision, modify or remove virtual machines
- Upload, create and manage virtual machine templates
- Add, modify, or remove segregated VDC internal networks
- Provision and manage virtual disks
- Modify the resource configurations for their virtual resources
- Power virtual machines on and off
- Access the virtual console of the virtual machine
- Manage virtual machine snapshots

Configuration changes not supported within the self-service portal can be submitted via Redcentric's change request process.

Customer templates or ISO images must contain required management agents and VMware tools. If not pre-installed, agents must be installed and configured as a post provisioning step by the customer, either manually or through customer managed automation. Please contact Redcentric support for the latest installation and configuration instructions.

1.7 Virtual Machine Specification

Customers are able to create virtual machines in any Broadcom supported configuration, up to the constraints of the host CPU, RAM, and Storage capacity with a suitable allowance for virtualisation overhead.

1.8 Virtual Machine Operating System

The platform supports any 64-bit server operating systems currently supported by the vendor, are not end of life and are on the [VMware Guest Operating System Compatibility Guide](#).

1.9 Over Subscription

Customers are able to configure an over-subscription ratio that is appropriate to their application demands, within the constraints of Broadcom best practice guidance. Assessing the performance impact is a customer responsibility. Redcentric do not provide a warranty for virtual machine performance.

1.10 Storage

Storage space is consumed by virtual machines' system disks, data and application disks, snapshots, templates, and swap files. These resources are consumed even if the disk is not allocated or visible to a virtual machine. Customers are responsible for removal of redundant snapshots and templates to release storage capacity for alternative usage.

1.11 Storage Performance

Evergreen Performance

Virtual disks and snapshots are held on high-performance solid-state storage and customers can expect up to 10 IOPS per allocated usable GB with an average response time of 3 – 5ms, based on 70/30 read/write split and 8KB transaction size. These targets are influenced by the customer I/O workload demands are not subject to an SLA.

Adopt Performance

Performance on adopted infrastructure will be subject to the constraints of the adopted storage architecture and the customer workload I/O demands.

1.12 Encryption at Rest

All data residing on storage supplied as part of the Evergreen offering is encrypted at rest using strong industry-standard encryption methods, ensuring that the platform is secure against physical data theft and supports many compliance requirements. Data is logically separated between environments, but is not zero-filled by default after deletion of the virtual storage.

Data is rendered unreadable upon server decommissioning.

Adopted storage that is not encrypted upon adoption will remain in an unencrypted state.

Secure destruction of storage adopted by Redcentric will be subject to additional charges if required

For further details see the off-boarding section 4.3.2.

1.13 Network access

External interfaces connect the provided host servers to other network resources, such as a customer WAN, Internet, or LAN. These network resources will be configured by the customer and Redcentric as part of the service activation. Connection to the external network allows the servers to co-exist within the customer's IP address scheme and be fully routable & integrated into the customer's network environment. Services on this platform will require connectivity for virtual machine session-based management and service access by the customer.

Network resources are defined during service delivery. Changes to the network topology can be requested throughout the lifetime of the service via the Account Manager. These changes may be subject to a one-off charge, and a design and planning lead time.

Virtual machines on the platform can be accessed in the following ways.

Access method	Description
Session Access	Session access is used to manage virtual machine operating systems. • Windows Server session via Remote Desktop Protocol (RDP) [subject to network access] • Linux Server Secure Shell (SSH) [subject to network access] • HTTPS access to configure virtual appliances with web-based configuration interfaces. Alternative session access methods can be provided subject to configuration of network access by the customer.
Console Access	Console access is provided for initial operating system configuration and fault finding when session access is not available. • Using a remote console application (download link provided) via the portal API • Using a web application within the self-service portal
LAN access	• Access from virtual and physical servers deployed by the customer on the same network segment
WAN/MPLS access	• Any server or device where the customer extends a WAN connection into the datacenter hosting the cloud platform, subject to network segregation and permitted access
Internet access	The virtual servers can be accessed from the Internet, Internet connectivity is provided by the customer. The customer is responsible for appropriate network security measures being in place.

2 RACI Matrix

The following tables device who is responsible, accountable, consulted, or informed in the execution of core service activities for both platform management and virtual resources consuming the platform.

2.1 Platform RACI

Activity	Redcentric	Customer
Physical datacentre operations (power, cooling, racks)	C	A/R
Data centre and rack security	C	A/R
All VMware by Broadcom licensing as agreed in the SoW (if any)	A/R	I
VMware platform management	A/R	C/I
Hardware lifecycle management (hosts, storage, switching) – applies to Evergreen offering only	A/R	I
Compute & storage configuration (Cloud platform side)	A/R	I
Storage provisioning (customer managed)	C	A/R
Network underlay management (DC switching, routing)	C	A/R
Internet availability (including DoS protection)	I	A/R
Connectivity to customer premises	I	A/R
Edge network & firewall policies	C	A/R
Active Directory / SAML configuration	A/R	C
VCF Organisation creation, including resource pools, 1st Org admin.	A/R	C
User Identity and Access Management within tenant.	I	A/R
Solution design / pre-sales	A/R	C
Platform monitoring (hypervisors, storage, clusters). External Storage monitoring is limited to connectivity and datastore consumption.	A/R	I
Network monitoring (WAN circuits, CPE)	I	A/R
Incident management — platform issues	A/R	C
Incident mgmt — connectivity issues	I	A/R

Activity	Redcentric	Customer
Backup & restore (customer provided solution integration to VCF)	A/R	C
Security — platform hardening	A/R	I
Security — edge/network controls	C	A/R
Patch mgmt — hypervisors & platform appliances	A/R	I
Compliance reporting — platform	A/R	I
Billing & usage reporting	A/R	I
Billing & invoicing to customers	I	A/R
Demand forecasting (planned capacity consumption)	C	A/R
Capacity reporting (platform)	A/R	I
Service roadmap & feature changes	A/R	I

A = Accountable, R = Responsible, C = Consulted, I = Informed

Please note that VMware Cloud Foundation terminology is subject to change and will be reflected in future iterations of this document.

2.2 Virtual Resource RACI

Activity	Redcentric	Customer
Reporting Microsoft license usage	I	A/R
Red Hat Enterprise licensing	I	A/R
Monitoring	I	A/R
Incident mgmt.	I/C	A/R
Backup & restore	I/C	A/R
Disaster recovery implementation	I	A/R
Disaster recovery testing and invocation	I/A	A/R
VM, Virtual Disk, Virtual network configuration	I/C	A/R
Network segregation	I/C	A/R
Tenant Organisation user configuration		A/R

Activity	Redcentric	Customer
Patch mgmt	I	A/R
VMtools installation	C	A/R
Anti-malware & anti-virus	I	A/R
Audit logging	I	A/R
SIEM integration	C	A/R
End-users relationship management	I	A/R

A = Accountable, R = Responsible, C = Consulted, I = Informed

2.3 Out of Scope Services

The following are outside of the scope of the Redcentric Partner Cloud service:

- Backup software licensing
- Backup infrastructure
- Disaster Recovery Replication software (unless Redcentric supported solution is subscribed to in an associated statement of work).
- External network capacity management
- Capacity forecasting

3 Software Licensing

Customers are responsible for ensuring that all software in use on the platform, except for software specified in the associated SoW, is properly licensed and used within the limitations on the licensing agreement. This includes ensuring that sufficient per-processor, -core, -user and -device licenses are in place and reviewed regularly to ensure continued compliance.

3.1 Licensing usage reporting

Customers are responsible for licensing and usage reporting of all licensed software installed on virtual machines or containers.

3.2 Software Licensing Compliance

In order to meet license compliance, customers must provide Redcentric with a copy of Microsoft SPLA usage reporting. This is solely to meet Redcentric's audit obligations.

4 Onboarding and Offboarding

4.1 Getting started

Redcentric will work with the customer to establish secure remote access to the customer site(s) where the cloud platform is deployed.

Customer must grant root level access to existing platform resources being adopted and any associated documentation.

Customers will provide details of authorised contacts for definition within Redcentric's ITSM tooling. Redcentric will grant access to tooling to enable service requests to be submitted.

Where Redcentric is providing the platform as part of the Evergeen offering, Redcentric will supply hardware and software as defined in the associate statement of work. Hardware and software shall be pre-configured by Redcentric based on design agreed with customer.

Customer will schedule site access, supported by required customer personnel to facilitate initial installation and setup.

A project plan detailing timescales will be agreed and documented following an initial project kick-off call.

4.2 Offboarding

4.2.1 End of contract data extraction

On termination or expiry of the Service Agreement, customers are responsible for the extraction on any data required beyond the end of the contract.

4.2.2 End of contract additional assistance

Where the customer requests additional transitional assistance, Redcentric shall provide such assistance as an additional service. The additional transitional assistance shall be chargeable at the Redcentric prevailing time and materials consultancy day rates.

4.2.3 Resource Deletion

The customer is responsible for deletion of virtual resources.

Redcentric will remove storage encryption keys to render data unreadable before server hosts are removed from service using nvme format commands via the ESX command line interface.

5 Service Levels and Service Credits

5.1 Incident Priority Definitions

The Cloud Services for Official use the following criteria for prioritisation of incidents

Priority	Contact Method	Criteria (Meets One or More)	Examples (Not a Definitive List)
P1	By Phone only	Severe unusable. Severe disruption of service or business functions, possibly with revenue loss. Critical Systems Unit failed or severely impaired. No workaround(s) exist. Affects Critical business unit, users, or functions.	Multiple server failures affecting key operational areas. Severe performance degradation. Financial systems affected in a close period. Security issue such as malware, virus.
P2	By Phone only	Causes major business disruption. VIP user(s) or Business Unit with significant reduction in system performance. No workaround(s) exist. Potential to cause or become a P1.	Slow response of key business application for one or more users. Security incident.
P3	email or customer portal	Impacts system availability or operation of services. Affects users within a single function. Workarounds may be in place. Business operations impacted but not severely.	Equipment failures which are covered by redundancy/ resiliency. Server or infrastructure device identified as not having current patch/pattern files within 5 days of a patch being uploaded to the distribution servers by Service Provider.
P4	email or customer portal	Minor disruption or usability issues. Affects single user or function. Workaround is available. Does not impact business operations.	Incident queries relating to Data Centre Services.

5.2 Incident Response and Resolution Targets

Incidents are responded to, resolved, and reported, according to the Key Performance Indicator (KPI) specifications as listed below

	Type	Service Level	Target	Measure
Response Time	KPI	Priority 1 (Critical)	15 min	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 2 (High)	30 min	
	KPI	Priority 3 (Medium)	60 min	
	KPI	Priority 4 (Low)	2 hrs.	
Resolution Time	KPI	Priority 1 (Critical)	4 hrs.	For each Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 2 (High)	8 hrs.	

	Type	Service Level	Target	Measure
	KPI	Priority 3 (Medium)	4 business days	
	KPI	Priority 4 (Low)	10 business days	
Updates	KPI	Priority 1 Incident	every hour (24x7)	Redcentric will contact the customer named contact by phone
	KPI	Priority 2 Incident	every 2 hours (24x7)	
	KPI	Priority 3 and 4	every 24 hours Mon-Fri	A Redcentric service desk incident assignee will email the customer named contact every 24 hours Monday to Friday with an update on incident status.
Reports	KPI	Priority 1 and 2	within 4 business days of incident resolution	Redcentric will formulate an incident report and present it to the customer service owner.

The provided times are targets, not guaranteed or warranted.

Despite the targeted timeframes provided above, Customer must provide primary support to their clients before receiving the support from Redcentric as detailed in this service definition. Customer is responsible for communicating incidents and resolution information received from Redcentric to Customer's clients.

6 Guaranteed availability

The Service Level applicable to Redcentric Partner Cloud is as follows

Service Level: Availability Measurement Period: Month	
Service Level	Not less than 99.95%

This service level applies solely to infrastructure running customer workloads. Portal and other tooling is excluded from downtime calculations.

Outages caused by failures by the customer to meet their responsibilities, including but not limited to power availability, cooling, and network availability are excluded from downtime calculations.

7 Lifecycle Management and Maintenance

Redcentric aim to provide 5 working days notice for standard changes that do not have the potential to impact performance or cause temporary loss of resilience for customer cloud assets.

Whilst the N+1 architecture for the production components is designed to eliminate any outages, some components may be offline whilst scheduled maintenance is carried out, in which case Redcentric will provide 14 days notice. Should a maintenance activity impact availability or performance of cloud assets consumed by customer applications, it will be scheduled between 11pm on Saturday and 5am on Sunday.

Maintenance for management tooling will be scheduled during normal office hours, any impact to availability of tooling will be advised in the change notification.

In the event of a high impact security or otherwise critical patch being released, Redcentric reserve the right to implement patching within 48 hours to protect the integrity of the service. An emergency notification will be provided in such circumstances. Redcentric will be the sole arbiter on the criticality of such emergency changes based on reasonable evaluation.

Redcentric will use reasonable endeavours to accommodate requests to defer planned changes where doing so would lessen the impact on the customer's business operations.

Customer is responsible for communication of change activities to their internal or external consumers.

8 Restrictions, Rights, Obligations, and Terms

Customer is prohibited from:

- 1) Re-selling the Services to a third party who is not the ultimate user of those services (unless expressly permitted in the SoW).
- 2) Excepting as expressly permitted in the SoW, permitting third party access to the Services (unless expressly permitted in the SoW).
- 3) Contracting with its clients to the extent that its obligations or rights in that contract are not permitted by Broadcom or would otherwise cause damage to Redcentric or would constitute a breach or cause a breach of this Service Definition, the SoW, or the MSA.
- 4) Installing Oracle software, including Java, unless confirmation to install that software has been signed and authorised by Redcentric in writing.
- 5) Causing or allowing damage to be caused to Redcentric's equipment or property (both real and intangible).
- 6) Utilising any shared resources provided by Redcentric excessively beyond fair use (fair use proportions will be determined by Redcentric, acting reasonably and considering the total number of users of the shared resources).

Customer must:

- 1) On its systems (particularly those which interact with the Services), maintain antivirus, anti-malware, local firewalls (including secure hardening rules), software and operating systems at the latest available version, and apply security vulnerability patches as soon as reasonably possible. The Customer must procure and enforce an equivalent obligation from its clients.
- 2) Prevent the occurrence of cyber attacks, transmission of viruses and malware, or the enabling of DDOS attacks, each to the extent that they can impact on the Services or the networks and tangible and intangible property of Redcentric. If any of those events occur, Customer must immediately notify Redcentric as soon as Customer becomes aware of the occurrence. The Customer must procure and enforce an equivalent obligation from its clients.
- 3) Accurately record and update the following metadata to be reported to Redcentric on the fifth Business Day of each month. This includes:
 - a) Microsoft usage for the previous month; and
 - b) Any and all additional metadata tagging and reporting requested by Redcentric.
- 4) Ensure that itself and its clients confirm that they will comply and do comply with Redcentric's acceptable use policy, any end user licence agreement that applies to the Services and Microsoft's acceptable use policy and applicable end user licence agreements.

- 5) Include in any of its marketing materials, documents, or contracts, reference to the Services (or derivation thereof as supplier by the Customer to its clients) as 'Powered by Redcentric'.
- 6) Maintain the following insurance coverage for the period of the SoW and for 6 years following that date.
 - a) £5,000,000 - employer's liability insurance;
 - b) £5,000,000 - public liability insurance;
 - c) £5,000,000 - personal injury insurance; and
 - d) £5,000,000 - cyber security insurance.

Both parties agree that the above coverage is a minimum and if greater coverage is held or more appropriate to reflect the prudent amount that would be insured by a reasonable board of directors, then the Customer must maintain or procure (as applicable) that higher amount of insurance cover.

The insurance policy must:

- (i) cover Redcentric as an additional insured;
- (ii) include a waiver of subrogation for additional insureds; and
- (iii) be primary to any policies held by additional insureds.

On request from Redcentric, Customer will provide certificates demonstrating the coverage required by this clause within 5 calendar days.

- 7) Provide notice to Redcentric of any planned or unplanned data centre or network maintenance (such notice to include the particulars of the work conducted and likely impact time) no less than 10 Business Days in advance of the maintenance.
- 8) Immediately inform Redcentric of any unplanned data center or network outages, providing reasonable details of the outage and likely time and/or plan for reestablishment of the data centre or network (as applicable)

Despite the terms of the MSA, the Customer indemnifies Redcentric for all claims, expenses, fines, penalties, damages, and costs incurred by the Customer's breach of the terms of this Service Definition. For this purpose of this indemnity, the limitations of liability within the MSA do not apply. The Customer will ensure that indemnity in this Service Definition is granted by its clients to the Customer and will procure that Redcentric may directly enforce the clients' indemnities.

Customer is responsible for all acts and omissions of its: (i) clients; (ii) parties it is responsible for; and (iii) those whom it permits to use the Services as if they were acts and omissions of the Customer.

Despite the terms of the MSA, if Customer breaches its obligations contained within this Service Definition, then Redcentric may immediately suspend or terminate the Services on prior written notice without liability to the Customer or any third parties. Customer will remain responsible for the payment of Charges for the Services during the period of suspension, or in the event of termination, Customer will pay to Redcentric the full Charges that would have been payable if the SoW had run until its term.

If Broadcom make changes to the partner programme that prevent or materially impair Redcentric's ability to deliver the Service to the Customer, Redcentric may, on prior written notice, terminate or suspend the agreement without liability to the Customer or any third parties.

Customer warrants that there will be no transfer of staff from the Customer (or any of its service providers) to Redcentric pursuant to the Transfer of Undertakings (Protection of Employment) Act 2006 for Redcentric's performance of the Services. If any staff are transferred, the Customer indemnifies Redcentric for all claims, losses, expenses, damages, legal fees, and any other consequences of the transfer without limitation, despite any limitations of liability in the Agreement.

Redcentric may at all reasonable times audit all documents and information applicable to the Services to verify the Customer's compliance with the terms of the Agreement, applicable laws, and both the Customer's and Redcentric's licencing conditions with third parties. Redcentric may take copies of the documents and information for its records. Customer must obtain an equivalent right of audit from its clients to facilitate Redcentric's

compliance with its obligations with the VMware licencing provider, Microsoft, or any other relevant party that oversees an aspect of the supply of the Services (whether directly or indirectly).

Any free value-add partner tools provided by Redcentric to Customer are provided as-is and without warranty or assumed liability, Redcentric may discontinue, downgrade, and vary any element of the value-add tools.

8.1 Backups & Disaster Recovery

Unless Customer also procures backup as a service, disaster recovery as a service, or other similar services from Redcentric, Redcentric has no responsibility for backups, disaster recovery, data loss, or availability of data.

8.2 Updates

Redcentric is the owner of the hardware used to deliver the Services. Redcentric will therefore determine the frequency and adoption of updates to the hardware (including the version of VMware or vSphere utilised on that hardware). Redcentric is also free to replace, wipe, and dispose of any hardware.

In the event of a major or minor version release by Broadcom, Redcentric may provide reasonable prior notice of no less than 14 calendar days, providing the details of the update and likely period for implementation. After those 14 calendar days, Redcentric may implement the relevant changes to the hardware.

Redcentric reserves the right to implement changes without notice and within timeframes that it decides to protect the integrity of the service – typically but not exclusively in response to a high-severity CVE being issued. If requested from Customer prior to upgrade or following, Customer will take all reasonable endeavours and offer reasonable assistance to Redcentric in the implementation or finalisation (as applicable) of the relevant change.

8.3 Discovery Burden

Customer is responsible for any failure to inform Redcentric of requirements for the Customer's client/s for an Agreement. Those requirements include bespoke design features and security clearances or accreditations required to deliver Services (whether directly or indirectly) to a particular client, including: Ministry of Defence, other government branches, and companies requiring PCI DSS.

Where Customer fails to disclose the requirements detailed above prior to contracting for the Services, any costs associated with obtaining the relevant design features, security clearances and/or accreditations, or any other requirements will be paid by the Customer.

8.4 Amendments

Despite any contrary provision within the SoW or MSA, Redcentric may change this Service Definition from time to time without Customer's consent. If Redcentric wants to implement a change, Redcentric will provide the Customer with at least 28 calendar days' prior written notice, including the details of the change. The change will become effective at the end of that notice period.

8.5 Definitions & Interpretation

Contract	means the MSA and the SoW.
Customer	means the party defined as such in the SoW.
End User	means any customer of the Customer to whom the Customer provides services which are enabled by, or dependent on, the Services
MSA	means the master services agreement referenced in the SoW.
Primary support	means first-line operational support provided in respect of the Services, including the initial receipt, logging, categorisation, prioritisation and diagnosis of Incidents and Service Requests, and the application of standard fixes or workarounds within the scope of the

	Services, together with coordination of escalation to Secondary Support where an issue cannot be resolved at first line.
Redcentric	means the party defined as such in the SoW.
Secondary support	means technical support provided in respect of the Services, involving in-depth investigation, diagnostics, remediation and configuration changes in relation to Incidents or underlying technical issues which cannot be resolved through Primary Support, including liaison with third-party vendors, licensors or manufacturers where required.
Service Definition	means this document.
SoW	means the Statement of Work between Redcentric and the Customer for the Services described in this Service Definition.
Staff	for the purposes of this Service Definition, the definition of Staff in the MSA is expanded to include any persons employed by an End User, or any servant, contractor, consultant, agent or supplier engaged by an End User, to the extent such persons are involved in activities connected with the Services or otherwise process Personal Data in connection with the Services.

Capitalised terms used in this Service Definition shall have the meanings given to them in the MSA.

Unless otherwise specified, the word “including” means “including without limitation”.

9 Service management

Redcentric will provide a centralised service management model for all services we deliver to you. Our proven model will ensure you receive service management and support services that is easily accessible and effective.

Our mature processes are based on the ITIL framework, fully supported by Gartner-referenced service management tools and process automation which ensures you receive a best-in-class user experience.

The proposed solution is inclusive of our support and account management service, which include

- Genuine 24/7/365 service desk which is manned, monitored and maintained using as mature ITSM tool

- Best-in-class secure management and monitoring tools, designed to ITIL guidelines.

Our service is underpinned by comprehensive, yet agile, documented processes that include major incident management. We have recently introduced enhanced SLAs within our support services, this means we will respond to you quicker and we are committing to faster fix times.

Service Reviews are an opportunity for us to collaboratively evaluate service performance and ensure it is effective and aligned to your needs. The service reviews seek to understand how we can work in partnership with you and your teams and to identify how we can improve performance. We work proactively to propose solutions to problems and suggest the best way to resolve any issues.



What happens at the monthly service review?

- Review service delivery using performance data and provide this in a graphical format
- Analyse support tickets to identify patterns that indicate we need to explore further to identify the root cause
- Review service availability, service exceptions, significant incidents and related trends
- Build operational relationships between our customers and the wider Redcentric team
- Seek to align internal resources within Redcentric to ensure effective service delivery
- Identify areas for improvement and include them in the service improvement plan
- Seek your input on how we can evolve our services to suit your future objectives
- Share our vision to demonstrate how we can support your future strategic aims
- Create and hold formal records in Redcentric's document management system

The monthly service pack provides a basis for discussion. It can be tailored to meet specific customer reporting needs as part of the onboarding process or within the lifetime of the contract. As standard, we provide a service pack that includes up to 12 months of data extracted from the support system and service monitoring systems. We analyse current and previous months' performance and identify any trends.

We operate a Service Management System which meets the requirements of ISO/IEC 2000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

Appendix 1 – Data Processing Statement

Scope 1 – Processing related to the Services

SCOPE OF PROCESSING	The receipt, storage, and disposal of data held on hardware which hosts virtual infrastructure provided as a service in the form of virtual machines utilising VMware technology.
CATEGORIES OF DATA SUBJECTS	- Customer's (and/or its Beneficiaries) Staff. - End User's: (i) Staff; and (ii) clients and other individuals whose personal data is recorded on the infrastructure provided as the Services, including individuals whose personal data is recorded on any platforms or applications operated within that infrastructure. The nature and categories of such data subjects are determined solely by the Customer or the End User.
TYPES OF CUSTOMER PERSONAL DATA	All information, including special category data, hosted in the infrastructure provided as the Services and any information held in any platforms or applications operated within that infrastructure (including data relating to End User's customers or other data concerning individuals that End User has a valid lawful basis for processing their information). Those types of information include and are not limited to: names, personal financial information, medical history and condition and other social information, details of trade union membership or criminal convictions. The nature and categories of such personal data are determined solely by the Customer or the End User.
SPECIAL CATEGORY DATA	Such special category data (as defined in Article 9) as may be recorded by the End User on the infrastructure which constitute the Services or applications and platforms hosted within that infrastructure, including, without limitation, medical information, criminal convictions, sex, sexual orientation, race or national origin. The nature and categories of such special category personal data are determined solely by the Customer or the End User.
NATURE OF PROCESSING	Receiving, storage and disposal.
PURPOSE OF PROCESSING	To provide infrastructure as a service in the form of virtual machines utilising VMware technology.
DURATION OF THE PROCESSING	The duration of the provision of the Services by the Redcentric Solutions Limited under the Services Agreement.

THIRD PARTY PROCESSORS	Redcentric Support Services Private Ltd Redcentric Data Centres Limited (and any successor to this company) RedRock Consulting Limited
TECHNICAL AND ORGANISATIONAL MEASURES FOR THE SECURITY OF CUSTOMER PERSONAL DATA	Redcentric Solutions Limited has no access to the personal data (special or otherwise) and therefore does not process it for company purposes, marketing, or otherwise. Any third party access is subject to a support agreement (e.g. infrastructure vendors) and duty of confidentiality. Redcentric Solutions Limited are certified to the following ISO standards:- ISO27001 - Information Security ISO9001 - Quality Management ISO20000 - Service Management ISO22301 - Business Continuity and Disaster Recovery ISO14001 - Environmental Management We are also Cyber Essentials and Cyber Essentials Plus certified Redcentric Solutions Limited data centres are physical site security certified to UK Gov data classification standard of OFFICIAL SENSITIVE for hosting. The Services are attested to PCI-DSS. Redcentric Solutions Limited operates 'secure-by-design' principles with least based privilege access across all products and services, operated documented development and testing lifecycles with approved security gates. For the purposes of its operations and not delivery of the Services, Redcentric Solutions Limited performs disaster recovery and resilience testing, risk assessment and treatment and operates a Business Continuity framework, including externally witnessed crisis management exercises. Redcentric Solutions Limited operates an information security management system using in-house dedicated personnel and assess and treat risks based on Confidentiality, Integrity and Availability across all information assets. Data is stored and transmitted to a minimum AES-256 encryption standard Redcentric Solutions Limited operates a Security Information and Event Management (SIEM) solution, intrusion detection and prevention methods, DDoS monitoring and protection software, multiple anti-virus, and anti-malware systems. Redcentric Solutions Limited Staff are trained across Information and Cyber Security, GDPR and Phishing regularly and staff vetting processes are in place where appropriate for some customers and services, with over 70% of technical personnel possessing UK Gov Security Clearance.
CONTACT DETAILS	Redcentric Solutions Limited: data.protectionofficer@redcentricplc.com Customer: as referenced in the MSA.

Scope 2 – Processing related to the management of the contract

SCOPE OF PROCESSING	The management of a contract concerning the receipt, storage, and disposal of data held on Redcentric Solutions Limited systems.
CATEGORIES OF DATA SUBJECTS	Customer's (and/or its Beneficiaries) Staff.
TYPES OF CUSTOMER PERSONAL DATA	Names, contact details (email addresses, telephone numbers) and IP addresses of the Customer's Staff and the End User's Staff.
SPECIAL CATEGORY DATA	None
NATURE OF PROCESSING	Receiving, storage and disposal.
PURPOSE OF PROCESSING	Administration of the contract, billing, and communication with the Customer.
DURATION OF THE PROCESSING	The duration of the provision of the Services by the Redcentric Solutions Limited under the Services Agreement and up to 7 years following the end of the Services for legal purposes.
THIRD PARTY PROCESSORS	Redcentric Support Services Private Ltd Redcentric Data Centres Limited (and any successor to this company)
TECHNICAL AND ORGANISATIONAL MEASURES FOR THE SECURITY OF CUSTOMER PERSONAL DATA	Redcentric Solutions Limited are certified to the following ISO standards:- ISO27001 - Information Security ISO9001 - Quality Management ISO20000 - Service Management ISO22301 - Business Continuity and Disaster Recovery ISO14001 - Environmental Management We are also Cyber Essentials and Cyber Essentials Plus certified

	Redcentric Solutions Limited data centres are physical site security certified to UK Gov data classification standard of OFFICIAL SENSITIVE for hosting. The Services are attested to PCI-DSS. Redcentric Solutions Limited operates 'secure-by-design' principles with least based privilege access across all products and services, operated documented development and testing lifecycles with approved security gates. For the purposes of its operations and not delivery of the Services, Redcentric Solutions Limited performs disaster recovery and resilience testing, risk assessment and treatment and operates a Business Continuity framework, including externally witnessed crisis management exercises. Redcentric Solutions Limited operates an information security management system using in-house dedicated personnel and assess and treat risks based on Confidentiality, Integrity and Availability across all information assets. Data is stored and transmitted to a minimum AES-256 encryption standard Redcentric Solutions Limited operates a Security Information and Event Management (SIEM) solution, intrusion detection and prevention methods, DDoS monitoring and protection software, multiple anti-virus, and anti-malware systems. Redcentric Solutions Limited Staff are trained across Information and Cyber Security, GDPR and Phishing regularly and staff vetting processes are in place where appropriate for some customers and services, with over 70% of technical personnel possessing UK Gov Security Clearance. Data retention policies are in place for corporate (B to B) data.
CONTACT DETAILS	Redcentric Solutions Limited: data.protectionofficer@redcentricplc.com Customer: as referenced in the MSA.



Proactive

We think and
act quickly



Inspired

We create
excitement through
innovation

Trusted

We do what
we say we will

Collaborative

We work together
to deliver
a common goal

Transparent

We are open,
honest and fair





Head office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED

