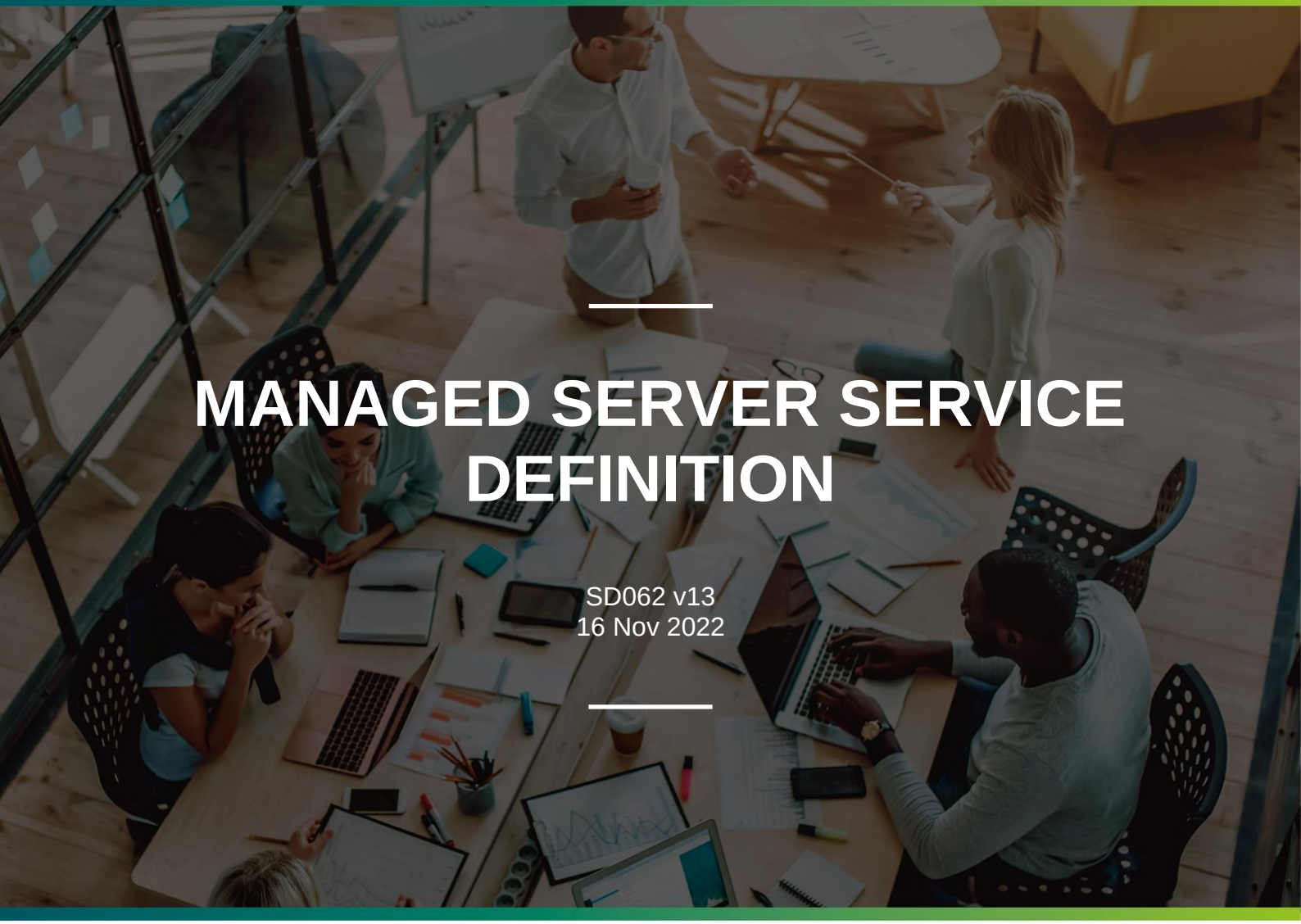

MANAGED SERVER SERVICE DEFINITION

SD062 v13
16 Nov 2022

redcentric

AGILE • AVAILABLE • ASSURED

1. Overview

The Managed Server service (MSS) provides access to Redcentric's support capability, technical skills and economies of scale, to manage the Customer's server operating systems deployed on Redcentric managed virtual or physical servers.

The standard service includes:

- Server operating system deployment
- Server operating system Customer for all managed servers on the shared platform
- Server monitoring
- Server operating system patching
- Anti-virus deployment and management
- Server availability management

2. Service description

2.1. Functionality

2.1.1. Supported Platforms

MSS supports the following operating system versions:

- Microsoft Windows Server 2019 Standard edition.
- Microsoft Windows Server 2016 Standard edition (Default Windows Server deployment). Note this excludes Core and Nano
- Microsoft Windows Server 2012 R2 Standard edition
- Red Hat Enterprise Linux 7 and 8
- CentOS 7
- Ubuntu 20.04 (LTS) & 22.04 (LTS) [1]
- Debian 10 (LTS) & 11[2]

Deployment on virtual or physical servers provided by Redcentric.

[1] Redcentric recommend the use of Ubuntu LTS releases, other releases will be supported on a reasonable endeavours basis when an extended support offering is subscribed to.
[2] Redcentric recommend the use of Debian LTS releases, other releases will be supported on a reasonable endeavours basis when an extended support offering is subscribed to.

2.1.2. Server Deployment

Redcentric will deploy the server operating system to a default best practice build on behalf of the Customer, when provisioning a new managed server.

Redcentric recommend a minimum managed server specification as detailed below:

OS	CPU Cores	RAM	Disk
Windows Server 2019	2	4GB	60GB
Windows Server 2016	2	4GB	60GB
Windows Server 2012	2	4GB	60GB
Red Hat Linux 7 & 8	2	4GB	60GB
CentOS 7	2	4GB	20GB
Ubuntu 20.04 LTS & 22.04 LTS	2	4GB	20GB
Debian 10 (LTS) & 11	2	4GB	20GB

2.1.3. Monitoring

Redcentric will connect the managed server to a Redcentric server management network using a dedicated network interface. Redcentric will monitor the server using a combination of SNMP and Windows Management Interface (WMI) for Windows servers.

Redcentric will monitor the managed server for:

Metric	Windows Server & Linux Server
Processor	Alert if processor exceeds a threshold over a set time period
Memory	Alert if memory exceeds a threshold over a set time period
Disk	Alert if usage exceeds a threshold over a set time period
Availability	Alert if the server does not respond to polling requests

Alerts generated by monitoring will automatically raise an incident within Redcentric's service desk. Redcentric will investigate the alert and corresponding fault, as detailed in the Remedial Action paragraph below.

Please note that SNMP must be installed and enabled on Linux systems to enable the service, where available SNMP V3 will be configured in preference to older versions..

2.1.4. Software Agents

Redcentric will install a software agent within managed server operating system for the following functions:

Software function	Windows Server	Linux Server
Antivirus	Agent installed	Agent installed
Patching	Agent installed	OS function
Backup (if taken)	Agent installed	Agent installed
Licence audit	Agent installed	Agent installed
Monitoring	OS function via WMI & SNMP	OS function via SNMP

2.1.5. Operating System Patching

Redcentric will only apply patches applicable to the managed server operating system. Redcentric will work with the customer during deployment of the managed servers to define patching groups and maintenance windows. Redcentric recommends following best practises and managed servers should be patched regularly, where practical ideally once a month and at most every three months.

The process for applying patches is as follows:

- Redcentric identifies available patches for each managed server and raises all appropriate changes
- Redcentric sends the patching report of patching groups and patches that will be installed on previously agreed date/times
- Customer reviews the patching report and informs Redcentric of any changes required i.e. patches not to be installed
- Redcentric carry out pre-patching activities prior to patching taking place
- Patches are applied and managed servers are rebooted
- Redcentric carry out post-patching checks and update customer on the completion status of the patching

Redcentric will work with the customer to make changes to the patching groups including additions, deletions, and amendments throughout the lifecycle of the service. Keeping managed servers patched and up to date is an essential requirement for the Managed Server Service.

Please note the following:

- If Redcentric are not informed of any changes to a scheduled patching group within the timescales below it will proceed with the patching
- If a customer wishes not to have any of the automatically approved updates applied, then they must inform Redcentric at least 24 hours before the scheduled start of the patching.
- If a customer wishes to amend a patching groups schedule this must be done 48 hours before the patching is scheduled to take place. If the customer requests changes within the 48-hour period before the patching is scheduled to start, then the patching should be suspended. Once the review has being completed the patching group will be re-scheduled.
- Any managed servers that are not patched on a minimum of a three-monthly cycle will not have an associated SLA.
- Unless Open-Source Operating Systems are subscribed to with a commercial support agreement, bug fixes and patches are subject to release by the Open-Source Community.
- Legacy Linux releases can be supported provided a then current Extended Long Term Support agreement is subscribed to.

Redcentric uses several third-party tools to patch Windows and Linux servers. Any additional infrastructure (Hardware, licenses etc.) required outside of the standard managed server service to provide patching will be chargeable to the customer.

2.1.6. Anti-virus

Redcentric will install, monitor and manage anti-virus software on each managed server. The anti-virus software used is provided by Sophos and is configured with the following functions:

- On access scanner: Scan executable, known vulnerable and file with no extensions on all drives
- Tamper control: Stop unauthorised configuration changes to the anti-virus software (Windows Server only)
- Device control: Block unauthorised external storage devices and wireless connection and short range access (Windows Server only)
- Exploit Prevention Model enabled
- Auto update: Check for update virus and malware definitions every 15 minutes

The Customer has no administrative access to the anti-virus software; all servers have the same Redcentric defined anti-virus protection. Redcentric will work with the Customer to implement the initial file exclusion list as part of the Service implementation.

Redcentric will terminate the SLA and not honour associated service credits if the Managed Server Service is affected by the Customer's disabling or removing anti-virus software.

2.1.7. Server Protection

Redcentric will protect the managed server, when delivered as a virtual server on Redcentric's Infrastructure as a Service, for the purposes of Redcentric being able to restore to an earlier working point if required as part of fault finding.

Server protection for physical servers will be done using the Redcentric MBS service which will take a daily backup of the system volume (OS) only, performed each night, and retained for 7 days, onsite to the managed server.

Server protection for virtual servers will be by storage snapshots (full server) performed each night, and retained for 7 days

Server protection is not a substitute for Customer performed backups as it does not provide:

- Granular file restoration
- Self-service access to the Customer to restore data
- Data retention beyond 7 days
- Offsite storage of backup data

Redcentric can provide a managed backup service to complement MSS.

2.1.8. Server Access

Redcentric allows the following access to the managed server.

Access method	Description
Console access	The managed server console can be accessed by a RDP session to a Windows server, or a SSH session to a Linux server.

2.1.9. Remedial Actions

Redcentric will perform remedial actions on the managed server where a fault is identified through monitoring. The objective of the remedial actions is to re-instate the managed server to a working state that includes:

- Managed server responding to monitoring agent
- Managed server monitored counters all below the alert trigger thresholds
- Managed server disks not full
- All automatic services running

To return the managed server to a working state, Redcentric will perform the following remedial actions:

- Notify the Customer upon detecting a fault with the managed server
- Investigate the fault and identify what steps are required. This could include:
  - Remove temporary files
  - Expand disk space
  - Restart the managed server, if the server is unresponsive
  - Restore the managed server from a previous protection point
- Coordinate remedial actions with the Customer, specifically where it is identified that a Customer application is at fault
- If necessary a rebuild to the managed server may be required to a default install

During out of hours periods, unless a server is unresponsive, Redcentric will record that the server is outside of normal operating parameters, but will not intervene. In the event that a critical threshold is reached Redcentric will contact customer personnel to agree remediation steps and intervene as directed.

A critical event is defined as:-

- Filesystem utilisation exceeds 94% (except where applications have pre-allocated space)
- CPU usage is sustained at 100% for 1 hour or more (exclusions for backup windows may apply)
- RAM usage exceeds 90% for a sustained period of 15 minutes or more (except where applications allocate all available RAM when working as designed)

2.1.10. Software Licensing

MSS includes the following software licences:

- Operating system licences for all managed servers on the shared platform
- Sophos anti-virus to be installed on the managed server (shared and dedicated hardware)
- Monitoring software used by Redcentric

Customer application licences are not included within MSS but can be provided as a separate licence charge via Redcentric's service provider licence agreements. Or under certain circumstances Customers may utilise their own licences under a licence mobility agreement.

Operating system licences for managed servers on dedicated hardware can utilise the Customer's existing licences or they can be provided as a separate chargeable item by Redcentric.

Customers migrating from an unmanaged service to the shared service will use Redcentric licences.

2.1.11. Server Accounts

Each managed server will be created in non-domain joined mode with local user and group accounts by default. The managed server can be deployed within an existing Customer domain if available.

In order to operate this Service Redcentric is required to have an administrator level account on the server for management and licence audit purposes.

2.1.12. Managed Server Location

Redcentric will provide MSS on servers provided on either Redcentric's infrastructure as a service, hosted physical server services, or Managed Public Cloud Services. For IaaS and hosted servers, the managed servers will be provided on equipment from within Redcentric's UK data centres. No access will be provided to the underlying physical infrastructure for monitoring, reporting or third-party hardware installations i.e., USB devices.

Where a Managed Public Cloud Service is subscribed to, Health monitoring of the Public Cloud infrastructure supporting the Managed Virtual Machines will be established and available to customers.

2.1.13. Server Hardening

The goal of hardening a system is to remove any unnecessary functionality and to configure what is left in a secure manner. Every application, service, driver, feature, and setting installed or enabled on a system can introduce vulnerabilities, especially if left at default settings.

However, there is no one size fits all solution – whilst there are guidelines/recommendations from bodies such as CIS these are just a suggestion, and each Customer/application may have specific requirements that can only be identified during the contract build/on-boarding phase. The Redcentric pre-sales team will work with Customers to provide advice on hardening as required during the sales process.

Server hardening is available for Customers on dedicated or shared hardware who are using Windows Server 2016 and later releases. At the start of a contract a Customer can choose either a standard or hardened OS. Both the standard and hardened OS are the same price at the start of a contract.

Redcentric provide both hardened and standard OS images for Linux.

The recommended approach for customers requiring hardened images is to start with a Centre for Internet WollSecurity (CIS) aligned build and then soften the security posture only when it is preventing the application from operating correctly. This aligns with the authorisation best practice to apply the least privilege principle,

If a customer initially chooses a standard OS and then at any point from initial deployment onwards decides to change to the hardened version a one-off Professional Services Charge will apply.

2.1.14. Operating System Upgrades

Redcentric will patch the server for the purposes of security and keeping it within a vendor supported level.

For major operating systems upgrades, for example Windows Server 2012 to Windows Server 2016, Redcentric's default approach is to provision a new server along the existing server, and allow the Customer to transfer applications, configuration, and data. Provisioning new servers may incur an additional charge in the following cases:

- Hosted Private Cloud – Typically Customers will utilise spare capacity within a dedicated platform, but if additional Hosted Private Cloud hosts are required a charge will be incurred for the platform upgrade
- Infrastructure as a Service – This is a usage service and additional servers will incur an additional Charge
- Hosted Physical Servers – A new Hosted Physical Server will be required to host the upgraded operating system

Redcentric can perform in-place operating system upgrades by exception to the above. This will incur an additional Charge to cover the plan, test and implement activities. It is expected that in-place upgrades will be performed out of hours for production Customer workloads.

2.2. Customer Dependencies

The following are Customer Dependencies for MSS.

- Provide a patching maintenance window for the managed server that includes a reboot if required
- Review and, if necessary, reject, patches to be applied to the managed server operating systems. Patch notification automatically generated 1 week before the agreed patching maintenance window
- Install, configure, license, and manage applications used on the managed server, such as IIS, Apache, DNS, MySQL, WINS, DHCP, etc.
- Define anti-virus exclusions required for the Customer's applications
- Allow Redcentric administrator level account on the managed server during the life of the service

2.3. Exclusions

The following are excluded from the scope of MSS.

- Reporting on performance metrics
- Backup or disaster recovery to a second data centre
- Patching of Customer applications not included within the Microsoft Windows update or Linux yum repositories
- Licensing of Customer applications
- Licensing of the operating system for managed servers on dedicated hardware is an option that the Customer can pay for, but is not provided by default
- Support of the Customer's applications
- Backup of the Customer's data to a second data centre, unless taken as part of a separate Redcentric service
- Recovery of the Customer's managed server to a second Redcentric data centre, unless taken as part of a separate Redcentric service
- Deleting files, other than temporary files, as part of remedial actions
- Active directory domain management (Windows Server only)
- LDAP system management
- Existing Customer server deployments cannot be brought into the scope of MSS

2.4. Roles and Responsibilities

The following table details roles and responsibilities that apply to MSS.

Task	Customer	Redcentric
Managed server administration		
Operating system support		✓
Day to day support / maintenance and incident resolution of each managed server		✓
Deployment of new managed servers on request of the Customer		✓
Implementation, configuration and maintenance of monitoring agent		✓
Implementation, configuration and maintenance of local server protection		✓
Storage management		
Disk management		✓
Storage area network (SAN) / network area storage (NAS) management (if applicable)		✓
Backups		
Install, operate and manage backup infrastructure	✓	
Ensure backup jobs are setup according to policy	✓	
Data restoration, such as individual files requests from end-users	✓	
Disaster recovery	✓	
Patching		
Review and assessment of available patches for managed servers and recommend to Customer which patches should be applied		✓
Approval of managed server patch implementation plan	✓	
Execution of managed server patch implementation plan		✓
Provide patch distribution infrastructure (e.g. Microsoft WSUS / yum repository)		✓
Monitoring		
Specify/confirm monitoring alarm thresholds		✓
Specify/confirm critical monitoring alarm thresholds	✓	
Implementation of monitoring agents and out-of-band data collectors		✓
Monitoring of alarms		✓
Capacity planning		
Own the capacity planning of the managed server	✓	
Identify potential performance bottlenecks for discussion at the service review	✓	✓
Discuss capacity change options	✓	✓
Approve capacity change options	✓	
Implement identified capacity recommendations		✓
Administration of user access and permissions		
Creation/management of administrative user accounts for access to managed server		✓
Request additional user access to the managed server	✓	
Availability management		

Monitor managed server availability		✓
Perform analysis where availability triggers a monitoring alert		✓
Remediate managed server to make managed server available		✓
Anti-virus management		
Installation, configuration, monitoring and management of anti-virus software		✓
Application management		
Installation, configuration, licensing, monitoring and management of application software	✓	

3. Implementation and Acceptance

3.1. MSS Implementation

Redcentric will deploy new managed servers as part of the Service delivery. By default this will include:

- Deployment of a managed server from an Redcentric template
- Patching to the latest available patch level
- Installation and configuration of anti-virus software
- Creation of a configuration item with Redcentric's configuration management database
- Setup of server monitoring
- Setup of server protection schedule
- Creation of local user accounts and groups
- Acceptance of the server into monitoring and support

Upon Service activation, the Customer will be able to access the managed server to install their applications. Additionally the Customer can engage Redcentric Professional Services to:

- Design and deploy Microsoft active directory domain for the managed servers
- Design and deploy Redcentric's managed backup service

The target lead time to complete Service delivery is detailed in the table below, for each Service element. This is subject to the timescales of delivery of the specific connection mechanism used to connect the Customer to MSS, such as delivery of Ethernet access circuits, NHS network (N3) connection, Internet address allocation via RIPE, firewall configuration, options selected, etc.

Service Element	Service Activation Timescales
MSS Implementation	Target completion within 20 working days

3.2. MSS Acceptance

The following are the Acceptance Criteria applicable to MSS:

- Verify that the primary Customer contact can access the managed server

The Customer will nominate (pre-installation) and make available an appropriately qualified representative to work with the Redcentric representative during the service delivery. The nominated Customer representative will accept delivery of MSS as a fully commissioned service and sign the service sign-off document and return this to Redcentric. The installation will be carried out between 09:00 - 17:30, Monday – Friday, except where agreed with the Customer.

4. Service Levels and Service Credits

4.1. Service Levels

The Service Level applicable to MSS is as follows:

Service Level: Availability Measurement Period: Month	
Service Level	Not less than the Service Level applicable to the underlying service on which MSS is provided

The following exclusions apply:

- Outages that are caused by OS bugs where no fix exists
- Outages that occur when a work-around or patch has been identified that has been notified to the customer but have not yet been implemented

4.2. Floor Service Level

The Floor Service Level applicable to MSS in respect of Availability shall be 85% in any given Month.

4.3. Service Credits

The Service Credits applicable to MSS shall be calculated as follows:

$$Service\ Credit = \frac{C\ x\ S}{MS}$$

Where:

S = the number of seconds by which Redcentric fails to meet the Service Level for Availability in the relevant Month

C = total Charges payable in respect of MSS for the same Month

MS = the total number of seconds in the same month

5. Data Processing

5.1. Data Processing Scope

- In the Managed Server Service (MSS) Redcentric is responsible for managing the operating system (OS) while the Customer is responsible for the application and the data.
- In terms of processing application data that is running on an application on a Redcentric managed OS, Redcentric does not materially access, alter or use the data.
- In terms of operating the IaaS service (which is commonly combined with the MSS), API commands are passed from the management portal to VMWare and associated supporting servers to orchestrate the build/management of virtual machines (VMs). It is Redcentric who issues these commands for a Managed Service, but these commands are creating the VMs and are not processing data. Please refer to section 5 of the Service Definition for IaaS for the data processing terms applicable to that Service.

5.2. Data Storage and Unencrypted Data

- No data is stored as part of the MSS. The Data Processing section (Section 5) of the Service Definition applicable to data storage will apply.
- If MSS is combined with IaaS, Redcentric stores log files of process workflows on the application server and database. Also log files are stored in vRealise Log Insights and vRealise Operations (both VMWare tools).
- Redcentric has access to unencrypted data because Redcentric has administrator rights to log-on to the server. However, in the normal course of business Redcentric has no reason to, and will not, access this data except in the course of providing support, which will be at the request of and in conjunction with the Customer.

5.3. Data Processing Decisions

- In the normal course of business Redcentric does not make any data processing decisions in relation to the Service. Processing is automated and instigated by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4. Service Configuration with Respect to Data

- The MSS is not configurable in a way that affects data processing decisions and outputs.
- The MSS manages the OS, and this does not involve configurations that affect Customer processing.

5.5. Data Backup

- MSS does not include a backup of application data in the sense of storing data off-site to provide a restore capability.
- MSS does however take a backup of the entire server (using either the Redcentric Managed Backup Service or by taking a 'snapshot image' which is stored on the local disc). This backup includes the OS, application and data - the objective is to create a backup that can be used to restore the server in the event of corruption or failure. This backup is not to be confused with a DR or off-site backup solution as this backup cannot be used for data restore purposes.
- In the normal course of business Redcentric will not access any data taken for server backup purposes except in the course of providing support, which will be at the request of and in conjunction with the Customer.

5.6. Sub-Processors

- No other parties are involved in delivering this service, and there are no sub-processors.

5.7. Customer Access to Data

- The Customer has direct access to the server (using VPN) and they have login rights that enable them to access, copy and process data as they wish.

5.8. Security Arrangements and Options

- The underlying services using MSS are hosted at Redcentric's datacentres with physical data centre security and cyber security measures (e.g. Firewall) in place to protect the back end systems and platforms.
- Access to the management server used to provide the MSS is restricted to Redcentric authorised support personnel.

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