

SPECIFIC CONDITIONS O1 – SSV MANAGEMENT SERVICES

These Specific Conditions govern the SSV Management Services that may be provided by the Company under a Contract, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms & Conditions for the Supply of Products and/or Services (the "**Conditions**"), which shall be deemed to be incorporated into the Contract for the performance of any SSV Management Services provided under these Specific Conditions.

1 DEFINITIONS

1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions only:

"Active Directory"	means the on-premises Windows server directory service from Microsoft that stores information about individual members of a domain, including devices and End Users, verifies their credentials and defines their access rights;
"Anti-Virus Management"	means the deployment of anti-virus software utilising the Virus Definitions in accordance with paragraph 4.4 of these Specific Conditions;
"Application Support and Management"	means the Services provided in accordance with paragraph 5 of these Specific Conditions;
"Backup Management"	means the Services provided in accordance with paragraph 4.5 of these Specific Conditions;
"Change"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Change Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Citrix"	means Citrix Corporation and its affiliates;
"Citrix XenDesktop"	means Citrix's desktop virtualisation software platform used to deliver virtual desktops;
"Critical Patch"	means a Patch designated by Microsoft as 'critical' upon its release or subsequently;
"Events"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Event Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Hypervisor"	means software that runs on computer hardware that allows one or more host computers to support multiple guest virtual machines by virtually sharing its resources;
"Incident"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Incident Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Managed Active Directory"	means the Services provided in accordance with paragraph 5.1 of these Specific Conditions;
"Microsoft"	means Microsoft Corporation and its affiliates;
"Microsoft Exchange"	means Microsoft's mail server and calendaring server software;
"Microsoft Remote Desktop Services"	means the components within Microsoft's Windows operating system based desktop virtualisation platform used to deliver virtual desktops;
"Microsoft Remote Desktop Client"	means Microsoft's client application software that allows end user devices to connect to the Remote Desktop Services;
"Operating System"	means the Microsoft Windows operating system software that manages computer hardware and software resources and provides common services for software and computer programs to run on the hardware;
"Patch"	means a component of software to fix issues or update computer software or its supporting data;
"Patch Management Service"	means the Services provided in accordance with paragraph 4.3 of these Specific Conditions;
"Problem Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Security Patch"	means a Patch that is released by Microsoft to address a security related issue;
"Service Request"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"SSV Management Services"	means the Services relating to servers, storage and virtualisation technologies provided in accordance with these Specific Conditions;
"Storage"	means network attached storage and/or storage area network devices;
"Storage Management"	means the Services provided in accordance with paragraph 4.6 of these Specific Conditions;
"Supported Equipment"	means the equipment and/or infrastructure in respect of which the Company is to provide the SSV Management Services to the Customer, as listed in the Order Form (including relevant descriptions and volumes);
"Supported Software"	means those Operating Systems, Hypervisors and any other software listed as supported software for the purposes of the SSV Management Services in the Order Form;
"Virus"	means any type of malware, virus, worm, Trojan horse, ransomware, spyware, adware, scareware or other computer program or software code that has been introduced into a system deliberately that carries out a useless and/or destructive function such as displaying an irritating message or systematically over-writing the information stored (that is, "infect" them) and spreads by contact between an infected program and an uninfected program; and
"Virus Definitions"	means the virus definitions provided by the anti-virus software provider and updated from time to time.

1.2 All other capitalised terms used in these Specific Conditions that are not defined in paragraph 1.1 have the meanings stated in the Conditions.

2 COMMENCEMENT DATE

2.1 The Commencement Date of the SSV Management Services shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of SSV Management Services to the Customer.

3 MINIMUM TERM

3.1 The Minimum Term for the SSV Management Services shall be as set out in the Order Form or, if no Minimum Term is specified, twelve (12) calendar months from the Commencement Date of the SSV Management Services.

4 SERVICE DELIVERABLES

4.1 Operating System Support

4.1.1 Where identified in the Order Form that the Company will provide support for any Operating System identified as Supported Software in the Order Form, it will:

- monitor Operating Systems in accordance with the Event Management process;
- resolve Incidents in accordance with the Incident Management process; and
- implement Changes to the Operating System in accordance with the Change Management process.

4.2 Hypervisor Support

- 4.2.1 Where identified in the Order Form that the Company will provide support for any Hypervisor identified as Supported Software in the Order Form, it will;
- (a) monitor the Hypervisor in accordance with the Event Management process;
 - (b) resolve Incidents in accordance with the Incident Management process; and
 - (c) implement Changes to the Hypervisor in accordance with the Change Management process.

4.3 Patch Management

- 4.3.1 Where the Company is providing Patch Management for the Supported Software and/or Supported Equipment as set out in the Order Form, it will do so exclusively using software determined by the Company. The Company reserves the right to change, at its cost, the Patch Management software from time to time at its sole discretion.
- 4.3.2 The Company will in respect of the Supported Software:
- (a) agree a monthly schedule with the Customer for Critical Patches and Security Patches to the Supported Software and deploy all Patches to the Supported Software in accordance with that schedule;
 - (b) manage the release of Critical Patches and Security Patches remotely as Changes;
 - (c) manage the application of Patches for any Hypervisor identified as Supported Software on release by the Vendor;
 - (d) when the Change is approved in accordance with the Change Management process, the Company will apply the approved Patches to the Customer's test environment or test infrastructure according to an agreed Patch schedule;
 - (e) where a test infrastructure does not exist or the Customer chooses not to have a test environment, the Company will use its reasonable endeavours to ensure that a reasonable back-out plan is available. However, the Company will not be liable for any interruption to service in the absence of a test environment or any other unintended consequences, loss or damage caused as a result of such interruption; and
 - (f) notify the Customer of any Critical Patches or Security Patches that are released that require action outside of the agreed Patching frequency, the installation of which will be managed as Changes; and
 - (g) where identified in the Order Form manage the application of Patches to Supported Software other than the Operating System and the Hypervisor, as set out in the Order Form.

4.4 Anti-Virus Management

- 4.4.1 Where the Company is providing Anti-Virus Management, as identified in the Order Form, it will:
- (a) do so exclusively using software determined by the Company and reserves the right to change, at its cost, the anti-virus software from time to time at its sole discretion, unless otherwise agreed in the Order Form;
 - (b) undertake the following scanning checks of the Operating System to seek to detect and clean away Viruses and to help protect files from the Viruses found in the Virus Definitions:
 - (i) on-access (as files are opened);
 - (ii) on-demand (a full scan requested as a Service Request); and/or
 - (iii) scheduled (a full scan at the frequency as set out in the Order Form or as otherwise agreed in writing by the parties);
 - (c) use reasonable endeavours to help block Viruses found in the Virus Definitions on detection;
 - (d) manage and apply updates to the Virus Definitions;
 - (e) perform configuration of anti-virus software; and
 - (f) where a Virus is found, use reasonable endeavours to take appropriate and reasonable measures to remove the Virus and recover the Operating System as far as reasonably possible to its last known good status as identified by the Company and notified to the Customer, including those applications covered by Application Support and Management.
- 4.4.2 The Company is not responsible for any data lost or corrupted or rendered inaccessible as a result of Virus outbreak or infection, or caused by misuse of any system or application by End Users or breach by End Users of any security policy.

4.5 Backup Management

- 4.5.1 Where the Company is providing Backup Management, as identified in the Order Form, it will:
- (a) do so using the Customer's relevant technology and/or software, as approved by the Company as set out in the Order Form or where expressly stated in the Order Form that the Company is supplying the technology and software, it will use such technology and/or software as determined by the Company. The Company reserves the right to change, at its cost, the Backup Management technology and/or software from time to time at its sole discretion;
 - (b) implement an agreed backup schedule;
 - (c) perform backups in accordance with the agreed backup schedule;
 - (d) notify the Customer where additional capacity for backups is required;
 - (e) fulfil Backup Management administration tasks as follows:
 - (i) monitoring backup progress; and
 - (ii) reviewing backup reports;
 - (f) in the event a backup has failed:
 - (i) use its reasonable endeavours to re-perform the failed backup within the same backup window, subject to backup schedule allowing;
 - (ii) report the failed backup to the Customer; and
 - (iii) investigate the failures in accordance with the Company's Incident Management process. In the event of a repeated failed backup, the Company will initiate Problem Management in accordance with the Company's Problem Management process; and
 - (g) implement Changes to the Backup Management in accordance with the Company's Change Management process.
- 4.5.2 Where the Backup Management technology and/or software is not expressly agreed to be provided by the Company in the Order Form, the underlying backup capacity and implementation is the Customer's responsibility.
- 4.5.3 In the event of loss of data that is subject to the Backup Management, the Company will restore the data to its last known good status as identified by the Company and notified to the Customer. This activity will be assigned a priority based upon its severity and managed via the Company's Incident Management process.
- 4.5.4 In the event that restoring the data requires the resources or assistance of the Customer or a third party supplier of the Customer, the Company will manage that resource in accordance with the Company's Incident Management and/or Problem Management process, as applicable.
- 4.5.5 The Company will not be responsible for loss or corruption of data, or lack of data consistency, relating to the performance of the Backup Management. In circumstances where data is lost or corrupted the Company's liability will be limited to using its reasonable endeavours to restore the previous most recent uncorrupted backup (if available) of such data.

4.6 Storage Management Services

- 4.6.1 Where identified in the Order Form that the Company will provide Storage Management in respect of any Supported Equipment comprising Storage devices, the Company will in respect of such Storage:
- (a) monitor the Supported Equipment and provide Event Management for any Events raised by this monitoring in accordance with the Event Management process;
 - (b) notify the Customer of any pre-agreed Events raised by the monitoring under paragraph 4.6.1(a);
 - (c) manage Incidents in respect of the Supported Equipment in accordance with the Incident Management process;
 - (d) implement Changes for the Supported Equipment in accordance with the Change Management process;
 - (e) provide reactive Problem Management for the Supported Equipment;
 - (f) for feature upgrades required by the Company, such updates may be identified by the Company or requested by the Customer. The Company will review firmware and software versions for Managed Equipment at least once a year to identify requirements for maintaining Vendor support. Feature upgrades requested by the Customer will incur additional cost on a time and materials basis, which will be agreed with the Customer prior to such work being completed;
 - (g) subject to paragraph 7 and where agreed by the Customer (such agreement not to be unreasonably withheld) update the firmware or software for the Managed Equipment;
 - (h) request repairs and/or replacement of Supported Equipment by liaising directly with the Vendor of the Supported Equipment and/or any third party as required to reinstate the Supported Equipment, provided that the Customer shall ensure that the Company is named as an authorised representative of the Customer where required on any Vendor or other third party support arrangement that has not been procured through the Company; and
 - (i) provide remote support relating to configuration and functionality of the software or firmware running on the Supported Equipment, which could include updates to the firmware or software to address stability issues or performance or functionality bugs, provided that any updates will be agreed with the Customer before being applied.

5 APPLICATION SUPPORT AND MANAGEMENT

5.1 Managed Active Directory

- 5.1.1 Where the Company is providing support and management for the Active Directory, as identified in the Order Form, it will:
- (a) monitor the Active Directory in accordance with the Event Management process; and
 - (b) perform Active Directory administration tasks as required from time to time in accordance with any relevant Change request from the Customer, comprising the following:
 - (i) creating computer objects;
 - (ii) renaming, moving and deleting computer objects within the Active Directory;
 - (iii) subject to paragraph 5.1.3 managing group policy objects and login scripts;
 - (iv) clearing local server cache as required;
 - (v) implementing automated scripts where appropriate; and
 - (vi) maintaining domain controllers within the domain in accordance with the Active Directory design.
- 5.1.2 The Company will perform Active Directory routine tasks comprising of the following:
- (a) maintaining subnets and sites to support the user login process;
 - (b) maintaining the global catalogue in the domain;
 - (c) backing up and recovering Active Directory data; and
 - (d) implementing Changes to the Active Directory in accordance with the Change Management process.
- 5.1.3 The Company is not responsible for the creation of any new Customer group policy as part of the SSV Management Services, unless agreed by the Company to be provided as an additional Service for additional Charges under this Contract.

5.2 Managed Microsoft Remote Desktop Services

- 5.2.1 Where it is identified in the Order Form that the Company is providing support and management for the Microsoft Remote Desktop Services component of the Operating System that is listed in the Order Form, it will:
- (a) monitor the Microsoft Remote Desktop Services component of the Operating System in accordance with the Event Management process;
 - (b) resolve Incidents in accordance with the Incident Management process;
 - (c) perform administration tasks for the Microsoft Remote Desktop Services component of the Operating System, as required from time to time in accordance with any relevant Service Request from the Customer.
- 5.2.2 The Customer acknowledges and agrees:
- (a) the Customer shall not have any elevated access (Administrator access) to enable file or application upgrades;
 - (b) the use of any unauthorised applications, processes or executable will be restricted;
 - (c) the Customer's ability to print & scan is limited to only those devices supporting the universal print driver at its current version, unless otherwise agreed in writing by the Company; and
 - (d) the Customer can only connect to the Microsoft Remote Desktop Services through devices supported by the current and latest version of the Microsoft Remote Desktop Client.

5.3 Managed Citrix XenDesktop

- 5.3.1 Where it is identified in the Order Form, that the Company is providing support and management for Citrix XenDesktop it will:
- (a) monitor the Citrix XenDesktop software in accordance with the Event Management process;
 - (b) resolve Incidents in accordance with the Incident Management process;
 - (c) perform administration tasks for the Citrix XenDesktop software, as required from time to time in accordance with any relevant Service Request from the Customer; and
 - (d) perform routine tasks for the Citrix XenDesktop software comprising of the following:
 - (i) update the virtual delivery agent (VDA) as updates are released by the Vendor, and;
 - (ii) run the base image script framework (BIS-F) following any update to master image.
- 5.3.2 The Customer acknowledges and agrees that:
- (a) the Customer shall not have any elevated access (Administrator access) to enable file or application upgrades;
 - (b) the use of any unauthorised applications, processes or executable will be restricted;
 - (c) the Customer's ability to print & scan is limited to only those devices supporting the universal print driver at its current version, unless otherwise agreed in writing by the Company; and
 - (d) the Customer can only connect to Citrix XenDesktop software through devices supported by the current and latest version of Citrix.

5.4 Managed Microsoft Exchange

- 5.4.1 Where it is identified in the Order Form that the Company is providing support and management for Microsoft Exchange, it will (provided always that the Customer's Microsoft Exchange remains a current version supported by Microsoft):
- (a) monitor the Microsoft Exchange in accordance with the Event Management process;
 - (b) resolve Incidents in accordance with the Incident Management process;
 - (c) perform administration tasks for the Microsoft Exchange, as required from time to time in accordance with any relevant Service Request from the Customer; and
 - (d) administer changes to the mail archive policy settings on request from the Customer in line with the Change Management process.

6 REPORTING

6.1 The Company will provide the following reports where the relevant Service is identified in the Order Form:

- 6.1.1 a Patch Management report, providing an overview of Patch Management in the reporting period, including:
- (a) status against most recent approved release;
 - (b) release success percentage; and
 - (c) devices below recommended currency;
- 6.1.2 an Anti-Virus Management report, providing an overview of Anti-Virus Management in the reporting period, including:
- (a) items held within the lost and found folder;
 - (b) decommissioned clients; and
 - (c) the percentage of devices with the correct version of the anti-virus software; and
- 6.1.3 a Backup Management report, providing an overview of the Backup Management in the reporting period, including:
- (a) total number of backups;
 - (b) daily overview;
 - (c) successful backups performed;
 - (d) failed backups; and
- 6.1.4 a Storage Management report in accordance with paragraph 6.2.

6.2 The Storage Management report will include data collated and analysed on a three monthly frequency to identify current, past and future projections of the Storage platform, as further detailed in Table 1 below.

6.3 All reports provided under this paragraph 6 will be distributed at the relevant frequency aligned to the relevant Service Management tier (as identified in the Order Form). Where no Service Management tier has been identified in the Order Form, the Company will not be obligated to provide any reporting identified in this paragraph 6.

Table 1 – Storage Management Service Reports

Report	Description of Report Content
Inventory	List the current Storage devices and components being monitored and included in the report. List those devices and components that have been removed since the last report.
System Health	Risks: List risks identified, and classified as High, Medium or Low. Identify those acknowledged, fixed or in progress and those that are not being actioned. Best Practice: List best practice configuration changes recommended and those not being actioned due to them not being relevant to the Customer Storage devices and/or configuration. Alerts: Highlight the alerts generated over the last 90 days and if there are any that are repeating themselves and need addressing. Software: Where the Storage system has a Storage operating system, identify the current version and the Vendor current version and provide upgrade advice based on minimum version for Vendor support, bug fixes and functionality enhancements. Firmware: Detail firmware versions running on the Storage devices. Identify the minimum versions required for Vendor support and highlight any relevant end of support dates. Recommend the proposed action to resolve any identified issues.
Storage Capacity and Trends	Overall Storage device capacity across the Supported Equipment, listing available and currently used capacity. Identify any Storage devices with greater than any agreed threshold for utilisation. Storage growth trends based on the last 90 days.
Storage Performance and Trends	CPU (central processing unit) utilisation levels within the Supported Equipment, including identifying any controller / node that exceeds any agreed thresholds for an extended period of time. Provide the volume (input/output per second) and the size (megabytes per second) of the disk requests per controller/node. If multiple protocols have been deployed, provide details for each protocol being used.

7 CUSTOMER OBLIGATIONS

7.1 The Customer will provide or otherwise comply with the obligations set out in this paragraph 7, which are Customer Obligations for the purposes of this Contract.

7.2 The Customer will:

- 7.2.1 ensure timely participation and engagement with the Change Management process and approve the requests submitted by the Company in accordance with the Change Management process and will not unreasonably withhold or delay such approval;
- 7.2.2 where the Company is providing Patch Management, the Customer will approve the requests submitted by the Company, in accordance with the Change Management process, and will not unreasonably withhold or delay such approval;
- 7.2.3 where the backup infrastructure is not on Sites that are under the control of the Company, the Customer must ensure that the infrastructure is suitably housed in accordance with Vendor's requirements, supply any tape media and load/unload such tape media from drives in accordance with the backup frequency;
- 7.2.4 provide a Windows server for the Company to use for the sole purposes of remote monitoring and/or management, which can be provided as a physical or virtual asset;

- 7.2.5 either:
- (a) allow for the set-up of a site to site VPN, or similar persistent connection as may be agreed in writing between the parties, to allow for remote monitoring and/or management by the Company, where the Company is agreeing to provide such connection as part of the Services, as set out in the Order Form; or
 - (b) provide and set-up a site to site VPN, or similar persistent connection as may be agreed in writing between the parties, to allow for remote monitoring and/or management by the Company, where it is not expressly set out in the Order Form that the Company is providing such connection;
- 7.2.6 at all times operate and maintain the Supported Software and Supported Equipment in a prudent manner and at all times in accordance with the Vendor's recommendations and operating manuals;
- 7.2.7 ensure that all Supported Equipment have relevant Vendor support purchased in order to ensure that the Company has access to the relevant Vendor software and firmware patches and updates on behalf of the Customer;
- 7.2.8 be responsible for obtaining and ensuring compliance with the terms of any software licence agreement for Supported Software and indemnify and hold the Company harmless against all claims, costs, damages or action arising as a result of any breach of such licence agreement and/or any infringement of any third party Intellectual Property Rights by the Customer or its End Users; and
- 7.2.9 remain responsible for the security and firewalls of the Customer's communications links, equipment, software, services and processes unless expressly agreed otherwise in this Contract as being provided by the Company.

8 EXCLUSIONS FROM THE SERVICES

8.1 The following are not included in the SSV Management Services:

- 8.1.1 additional services arising due to:
- (a) server maintenance or application maintenance carried out by the Customer or any incorrect or unauthorised use of the Supported Software by the Customer or its End Users;
 - (b) any modifications or customisation of the Supported Software not authorised in writing by the Company, including but not be limited to changes to the logical or physical database schema for the Supported Software, changes to the disk layout and configuration, and/or hand-modified changes to the data within a database;
 - (c) any disruption of service through the introduction of a Virus;
 - (d) any failure due to environmental conditions onsite;
 - (e) any failure due to loss of power to the Supported Equipment;
 - (f) any act or omission of Microsoft;
- 8.1.2 any software other than the Supported Software and/or any programs or application used in conjunction with the Supported Software;
- 8.1.3 any performance management of third party break-fix maintenance providers. The Company will take on the responsibility of passing the relevant information to the third party break-fix maintenance providers but the Company cannot manage that suppliers responsibilities to meet the service levels offered to the Customer; and/or
- 8.1.4 the cost of any software license renewals or security certificate renewals or the provision or installation of any hardware, licensing and/or security certificates that are required to meet the pre-requisites for any upgrades released by the Vendor of the Supported Software;
- 8.1.5 management connectivity between the Supported Equipment and the Company;
- 8.1.6 any application packaging or distribution or any application version changes that require repackaging and testing and/or redistribution before release into the Microsoft Remote Desktop Services or Citrix XenDesktop, unless expressly agreed otherwise in this Contract as being provided by the Company;

and the Company reserves the right to levy additional Charges on a time and materials basis in respect of any such additional Services requested by the Customer from time to time.

- 8.2 The Company does not guarantee the effectiveness of any Virus Definitions. The Company is not responsible for the Virus Definitions not including a specific Virus.
- 8.3 Non-critical Patches that are required outside the standard monthly patch cycle for critical and security Patches (including feature upgrades and updates) and/or major version upgrades will be released as agreed with the Customer as additional Services on a chargeable basis.
- 8.4 The SSV Management Services do not include requests for basic product training or technical consulting.
- 8.5 The Company reserves the right to refuse or withdraw SSV Management Services for any Supported Software that is or that falls outside of the relevant Vendor support during the Term of this Contract. Alternatively, where agreed in writing between the parties, the Company may continue to be provided Services on a reasonable endeavours basis.

9 CHARGES

- 9.1 The Charges for the SSV Management Services are as identified in the Order Form.
- 9.2 Unless otherwise provided in the Order Form, the Company is entitled to invoice for the SSV Management Services monthly in advance, with the first invoice issued by the Company on or around the Commencement Date.

10 SERVICE LEVELS

- 10.1 The Company will supply the SSV Management Services in accordance with the applicable Service Levels set out in Specific Conditions X3 – Standard Operational Services.