## SPECIFIC CONDITIONS I3 – CLOUD MANAGEMENT SERVICES

These Specific Conditions govern the Cloud Management Services that may be provided by the Company under an Order Form, 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**"),Specific Conditions X3 – Standard Operational Services and Specific Conditions F2 – Service Management, which shall be deemed to be incorporated into the Contract for the performance of any Cloud Management Services performed 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; |
| "Administrator Access" | means accounts with the ability to modify computer hardware and operating system settings, which are above the level of a user's abilities on the given system; |
| "Application Support and Management" | means the Services provided in accordance with paragraph 5 of these Specific Conditions; |
| "Azure" | means the virtual public cloud offering provided by Microsoft called Azure; |
| "Azure Active Directory" | means a multi-tenant directory service from Microsoft that offers authentication, identity management and access capabilities for applications running in Azure together with applications running in an on-premises environment; |
| "Azure Advisor Optimisation Checks" | means the Services provided in accordance with paragraph 6.6 of these Specific Conditions; |
| "Azure Management Services" | means the Services provided in accordance with paragraph 6 of these Specific Conditions; "Azure Portal" means the Microsoft owned and managed web browser through which the Customer may access Azure, found at portal.azure.com or any other web browser notified by the Company or Microsoft to the Customer from time to time; |
| "Azure Security Center Review" | means the Services provided in accordance with paragraph 6.5 of these Specific Conditions; |
| "Azure Services" | means the online services within Azure provided by Microsoft to the Customer (if any); |
| "Azure Site Recovery (ASR)" | means Microsoft's software provided to orchestrate and automate replication of virtual machines between Azure regions; on-premises machines and physical servers to Azure and/or on-premises machines to a secondary data centre; |
| "Azure Workload Power Management" | means the Services provided in accordance with paragraph 6.7 of these Specific Conditions; |
| "Backup Management Services" | 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; |
| "Cloud Management Services" | means the Services provided by the Company to the Customer in accordance with these Specific Conditions; |
| "Complex COTS" | means COTS which are deemed by the Company to be moderate or high risk with a complex Rollback process; |
| "COTS" | means commercial off the shelf software, which isa software product that is commercially ready-made and available for sale, lease, or license to the general public; |
| "Critical Patch" | means a Patch designated by the Vendor as 'critical' upon its release or subsequently; |
| "Cumulative Patch" | means a Patch which includes previously released updates and designated by the Vendor as 'Cumulative'; |
| "Cyber Threat" | means any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service; |
| "Disaster Recovery Invocation" or "DR Invocation" | means the Services provided in accordance with paragraph 4.6.3 of these Specific Conditions; |
| "Disaster Recovery Invocation Plan" or "DR Invocation Plan" | means a document which may include but not be limited to supported cloud environment topology, supported networking topology, the order of power on procedures for services and authorised Customer contact details; |
| "Disaster Recovery Services" or "DR Services" | means the Services provided in accordance with paragraph 4.6 of these Specific Conditions; |
| "Disaster Recovery Simulation Test" or "DR Simulation Test" | means the Services provided in accordance with paragraph 4.6.2 of these Specific Conditions; |
| "Disaster Recovery Simulation Test Plan" | |

| | |
|---|---|
| or "DR Simulation Test Plan" | means a document which may include but not be limited to authorised Customer contact details, supported cloud environment topology, supported networking topology, the order of power on procedures for services; |
| "EDR" | means Endpoint Detection and Response, a next-generation version of anti-virus which continually detects and mitigates Cyber Threats on servers and endpoints; |
| "EDR Management" | means the deployment and utilisation of EDR software to detect and respond to Cyber Threats in accordance with paragraph 4.4 of these Specific Conditions; |
| "End of Support Date" | means the date beyond which the Vendor will no longer provide software support in relation to the Supported Software including, but not limited to, feature updates, security updates, incident support, integration support and licencing; |
| "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; |
| "Feature Patch" | means a Patch that is released to add new functionality to the software; |
| "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; |
| "IaaS" | means infrastructure as a service; |
| "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; |
| "Malicious Content" | means any type of malware, ransomware, spyware, adware, scareware, virus, worm, Trojan horse, or other computer program or software code used to disrupt computer operation, gather sensitive information, or gain access to private computer systems; |
| "Managed Active Directory" | means the Services provided in accordance with paragraph 5.1 of these Specific Conditions; |
| "Managed Azure Active Directory" | means the Services provided in accordance with paragraph 6.2 of these Specific Conditions; |
| "Managed Resource Groups" | means the number of Resource Groups that will be managed by the Company as part of the Cloud Management Services, as set out in the Order Form; |
| "Managed Subscription Service" | means the Services provided in accordance with paragraph 6.3 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; |
| "Microsoft SCCM" | means Microsoft's System Center Configuration Manager; |
| "Microsoft SQL" | means Microsoft's database application based on the structured query language and distributed by Microsoft; |
| "Non-Microsoft SQL" | means a database application based on the structured query language and distributed by a Vendor other than Microsoft; |
| "Legacy System" | means a system which has reached the End of Support Date as notified by the Vendor; |
| "Legacy System Support" | means the Cloud Management Services provided in relation to a Legacy System, where specified in the Order Form; |
| "Operating System" | means the operating system software that manages the Customer's computer hardware and software resources and provides common services for software and computer programs to run on the hardware; |
| "PaaS" | means platform as a service; |
| "Patch" or "Patching" | means a component of software to fix issues or update computer software or its supporting data; |
| "Patch Management" | means the Services provided in accordance with paragraph 4.33 of these Specific Conditions; |
| "Problem Management" | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| "Resource Group" | means any collection of related resources (including virtual machines, databases and other assets) added to Azure, that is created and used to manage permissions, set alerts and manage billing for that collection; |
| "Rollback " | means the returning of the Supported Cloud Environment to the original live state of configuration that was in place before the DR Invocation Plan was enacted; |
| "Rollup Patch" | means a Patch which includes multiple patches combined into a single update and designated by the Vendor as 'Rollup'; |
| "Sandbox Environment" | means an isolated Customer environment of a suitable size to support testing as stipulated in the Disaster Recovery Simulation Test Plan; |
| "Security Incident" | means an event indicating that the Supported Cloud Environment may have been breached or compromised through the presence of Malicious Content and/or a Cyber Threat evidenced by the EDR software; |
| "Security Patch" | means a Patch that is released to address a security related issue; |

| | |
|---|---|
| "Service Request" | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| "Simple COTS" | means COTS which are deemed by the Company to be low risk with a simple Rollback process; |
| "SSL Certificates" | means secure sockets layer (SSL) certificates, which are the small data files that digitally bind a cryptographic key to an organisation's details to enable an encrypted connection between a browser or user's computer and a server or website; |
| "Storage" | means network attached storage and/or storage area network devices; |
| "Storage Management" | means the Services provided in accordance with paragraph 4.8 of these Specific Conditions; |
| "Supported Cloud Environment" | means any virtual public, private or hybrid cloud environment that is hosting or supporting IaaS, PaaS and/or SaaS for the Customer that may comprise some or all of the following: (i) Azure Services; (ii) DaisyCloud Flex Services, where provided by the Company in accordance with this Contract and/or (iii) cloud services provided by any other third party public or private cloud services provider, and as identified in the Order Form as the Supported Cloud Environment; |
| "Supported Equipment" | means the equipment and/or infrastructure in respect of which the Company is to provide the Cloud Management Services to the Customer, as listed in the Order Form(including relevant descriptions and volumes); |
| "Supported Software" | means the Operating System and/or any other software listed as supported software on the Order Form for the purposes of the Cloud Management Services; |
| "Subscription" | has the meaning given to it in Specific Conditions I1 – Microsoft Cloud Services; |
| "System Rebuild" | means the rebuilding of the Supported Software to a basic configuration; |
| "System Restore" | means the restoration of the Supported Software to that of a previous point in time |
| "Unmanaged Resource Groups" | means any Resource Group that is not a Managed Resource Group; and |
| "Vendor Support" | means services provided by the Vendor in relation to the Supported Software such as management, development, integration, security, licensing maintenance and training services. |

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, Specific Conditions X3 – Standard Operational Services and/or Specific Conditions F2 – Service Management.

## 2 COMMENCEMENT DATE

2.1 The Commencement Date of the Cloud 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 the Cloud Management Services to the Customer.

## 3 MINIMUM TERM

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

## 4 SERVICE DELIVERABLES

4.1 **Operating System Support**

4.1.1 The Company will:

(a) monitor Operating Systems in accordance with the Event Management process;

(b) resolve Incidents in accordance with the Incident Management process; and

(c) implement Operating System Changes 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 Supported Software and/or Supported Equipment, as identified in the Order Form, it will:

(a) apply Patches to the Supported Software in the Supported Cloud Environment only, 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;

(b) manage the release of all Patches remotely as Changes;

(c) when the Change is approved in accordance with the Change Management process, apply the approved Patches to the Customer test environment or test infrastructure according to an agreed Patch schedule;

4.3.2 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;

4.3.3 Where the Company is providing Operating System Patching, as identified in the Order Form, it will in respect of the Supported Software:

(a) agree a monthly Patching schedule with the Customer for Rollup Patches and Cumulative Patches related to the Supported Software and deploy all Patches to the Supported Software in accordance with that schedule; and

(b) notify the Customer of any Critical Patches and Security Patches that are released by the Vendor that require action outside of the agreed Patching frequency, the installation of which will be managed as Changes.

4.3.4 Where the Company is providing Simple COTS Patching, as identified in the Order Form, it will in respect of the Supported Software:

(a) agree with the Customer a Simple COTS list to be to patched and specified in the Service Operations Manual as the Simple COTS list; and

(b) notify the Customer of any Security Patches and Feature Patches that are released by the Vendor and deploy all Patches to the Supported Software under the process for a Standard Change.

4.3.5 Where the Company is providing Complex COTS Patching, as identified in the Order Form, it will in respect of the Supported Software:

(a) agree with the Customer a Complex COTS list to be to patched and specified in the Service Operations Manual as the Complex COTS list; and

(b) notify the Customer of any Security Patches and Feature Patches that are released by the Vendor and deploy all Patches to the Supported Software under the process for a Normal Change;

4.4 **EDR Management**

4.4.1 Where the Company is providing EDR Management, as identified in the Order Form, it will:

(a) do so exclusively within the Supported Cloud Environment using EDR software determined by the Company and reserves the right to change, at its cost, the EDR software from time to time at its sole discretion, unless otherwise agreed in the Order Form;

(b) utilise the EDR software to continuously monitor the servers within the Supported Cloud Environment to detect and mitigate Malicious Content and/or Cyber Threats;

(c) investigate potential security incidents and:

(i) where a Security Incident is identified, take appropriate and reasonable measures to remediate the Security Incident using the capabilities of the EDR software; or

(ii) where a Security Incident cannot be remediated using the capabilities of the EDR software, recover the Operating System as far as reasonably possible to its last known good configuration as identified by the Company and notified to the Customer;

(d) manage and apply updates to the EDR software; and

(e) perform configuration of the EDR software in accordance with good industry practice and Vendor guidelines.

4.4.2 The Company is not responsible for any data lost or corrupted or rendered inaccessible from the Supported Cloud Environment or otherwise as a result of any Security Incident, or caused by misuse of any system or application hosted in or connected to the Supported Cloud Environment by End Users or breach by End Users of any security policy.

4.5 **Backup Management Services**

4.5.1 Where the Company is providing Backup Management Services into or otherwise in connection with the Supported Cloud Environment, as identified on the Order Form it will:

(a) do so using technology and software determined by the Company or using the Customer's relevant technology and/or software where this has been approved in writing by the Company and the Company reserves the right, at its cost, to change the Backup Management Services 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 Services 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 Services in accordance with the Company's Change Management process.

4.5.2 Where the Backup Management Services technology and/or software is not expressly agreed to be provided by the Company, 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 Services, 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 in accordance with 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 third party 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 Services. 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 **Disaster Recovery Services**

4.6.1 Where the Company is providing DR Services within the Supported Cloud Environment, as identified in the Order Form it will:

(a) work with the Customer in a workshop to define a DR Simulation Test Plan and DR Invocation plan applicable for the Supported Cloud Environment;

(b) store the DR Test Plan and the DR Invocation plan in the Service Operations Manual;

4.6.2 Where the Company is providing a DR Simulation Test, as identified in the Order Form it will:

(a) enact the DR Simulation Test Plan annually on a mutually agreed date; and

(b) update the DR Simulation Test Plan following the DR Simulation Test with technical or process improvements identified during the testing and agreed with the Customer.

4.6.3 Where the Company is providing DR Invocation, as identified in the Order Form it will:

(a) enact the DR Invocation Plan upon appropriate Customer authority as documented within the DR Invocation Plan; and

(b) provide a quotation for the Rollback of services to be performed at a mutually agreed date.

4.6.4 The Customer acknowledges and agrees that:

(a) the Customer shall provide a suitable Customer Representative in order to participate in the workshops referenced in paragraph 4.6.1(a) and agree the Disaster Recovery Simulation Test Plan and the Disaster Recovery Invocation Plan;

(b) the Customer shall provide a suitable Customer Representative to enact the DR Simulation Test Plan during the Disaster Recovery Simulation Test;

(c) the Customer shall provide a suitable Customer Representative to authorise DR Invocation;

(d) a DR Simulation Test without adverse impact to live services is reliant upon a Customer Sandbox environment of a suitable size to support the replication of the Supported Software; and

(e) Rollback of DR Services following a DR Invocation is performed on a chargeable basis, a time and materials quotation will be provided by the Company to the Customer for acceptance;

4.7 **SSL Certificates**

Where the Company is managing SSL Certificates in connection with the Supported Cloud Environment, as identified in the Order Form, it will procure and install SSL Certificates from a reputable Certificate Authority, which will be to 2048 bit SSL with 256 bit encryption and SHA2 standard, subject to the Customer paying any third party costs associated with the procurement, renewal or registration process of any additional SSL Certificates.

4.8 **Storage Management Services**

4.8.1 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 4.8.1(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) identify feature upgrades as necessary. . The Company will review firmware and software versions for Supported Equipment at least once a year to identify requirements for maintaining Vendor support. Feature upgrades requested by the Customer will incur additional charges on a time and materials basis, which will be agreed with the Customer prior to such work being completed;

(g) subject to paragraph 9 and where agreed by the Customer (such agreement not to be unreasonably withheld or delayed) update the firmware or software for the Supported 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 Managed 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 Company's 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 creating any new Customer group policy objects or changing any Customer group policy objects as part of the Cloud Management Services, unless agreed 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 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 and 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; and

(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.

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 and 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.

5.5 **Managed Microsoft SQL**

5.5.1 Where it is identified in the Order Form that the Company is providing support and management for Microsoft SQL, it will (provided always that the Customer's Microsoft SQL remains a current version supported by Microsoft):

(a) monitor the Microsoft SQL in accordance with the Event Management process;

(b) resolve Incidents in accordance with the Incident Management process;

(c) perform administration tasks for the Microsoft SQL, as required from time to time in accordance with any relevant Service Request from the Customer; and

(d) administer changes to the Microsoft SQL settings on request from the Customer in line with the Change Management process.

5.6 **Managed Non-Microsoft SQL**

5.6.1 Where it is identified in the Order Form that the Company is providing support and management for Non-Microsoft SQL, it will (provided always that the Customer's Non-Microsoft SQL remains a current version supported by Microsoft):

(a) monitor the Non-Microsoft SQL in accordance with the Event Management process;

(b) resolve Incidents in accordance with the Incident Management process;

(c) perform administration tasks for the Non-Microsoft SQL, as required from time to time in accordance with any relevant Service Request from the Customer; and

(d) administer changes to the Non-Microsoft SQL settings on request from the Customer in line with the Change Management process.

5.7 **Managed Microsoft SCCM**

5.7.1 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 SCCM remains a current version supported by Microsoft):

(a) monitor the Microsoft SCCM in accordance with the Event Management process;

(b) resolve Incidents in accordance with the Incident Management process;

(c) perform administration tasks for Microsoft SCCM, as required from time to time in accordance with any relevant Service Request from the Customer; and

(d) administer changes to the Microsoft SCCM settings on request from the Customer in line with the Change Management process.

## 6 AZURE SPECIFIC CONDITIONS

6.1 Where the Company is providing Cloud Management Services for Azure Services, as identified on the Order Form, the terms in this paragraph 6 shall also apply.

6.2 **Managed Azure Active Directory**

6.2.1 The Company will:

(a) configure replication between the Customer's Active Directory and the Azure Active Directory utilised for administration and for the Managed Subscription Services;

(b) perform Azure Active Directory administration tasks as required from time to time in accordance with any relevant Change request by the Customer, comprising the following:

(i) managing the Customer's Azure Active Directory replication policy in accordance with Microsoft guidelines;

(ii) restricting permissions for accounts within Azure and Office 365 via role-based administration based upon Microsoft guidelines and built-in roles;

(iii) administering adds, moves and changes to objects within the Azure Active Directory to maintain the working replication necessary between Azure Active Directory and Active Directory; and

(iv) monitoring the replication of information between the Active Directory and Azure Active Directory in accordance with the Event Management process.

6.3 **Managed Subscription Services for Azure**

6.3.1 The Company will perform the following administration tasks:

(a) manage the electronic ordering and administration of Subscriptions relevant to the Azure Services;

(b) manage usage quotas or subscription limits to help ensure suitable availability of resources and capacity within the Azure Services; and

(c) upon request supply the Customer with a reconciliation file of Azure Services usage-based Subscriptions and licence-based Subscriptions for a defined period.

6.3.2 The Customer will not have direct access to the Subscriptions and billing sections of the Azure Portal. The Company may at its discretion from time to time make available to the Customer direct access to a subscriptions and billing portal through a relevant interface. The Customer acknowledges and agrees, that the Company makes no promise, guarantee or commitment to do so, or to maintain access to such portal, if provided.

6.3.3 The Company will hold the administrative rights for the Subscriptions (including the tenancy for such Subscriptions) during the term of the Contract.

6.3.4 The Company will, unless otherwise agreed in writing:

(a) configure Active Directory accounts with read-only role-based access control to the Azure Portal for Managed Resource Groups; and

(b) configure Active Directory accounts with read-write role-based access control to the Azure Portal for Unmanaged Resource Groups.

6.4 **Azure Site Recovery Management**

6.4.1 The Company will:

(a) resolve ASR Incidents in accordance with the Company's Incident Management process;

(b) implement ASR Changes in accordance with the Company's Change Management process;

(c) fail over the Azure Services using ASR in the event of a primary site failure; and

(d) reconfigure the ASR replication to a new secondary site post fail over.

6.5 **Azure Security Center Review**

6.5.1 Where the Company is providing Azure Security Center Review, as identified on the Order Form, it will:

(a) perform a monthly check of Azure Security Center to review secure score and recommendations made by Azure Security Center;

(b) log all outstanding recommendations as tasks for resolution and assign to the correct resolver group or to the Service Management resolver group; and

(c) where a recommendation requires input from the Customer for reasons of cost, complexity or when considered a project task, raise a task for each recommendation. Service Management will discuss and agree with the Customer which of the recommendations should be progressed and follow the necessary process to allow recommendations to be implemented.

6.6 **Azure Advisor Optimisation Checks**

6.6.1 Where the Company is providing Azure Advisor Optimisation Checks, as identified on the Order Form, it will:

(a) perform a weekly check of Azure Advisor to review recommendations made by Azure Advisor;

(b) log all outstanding recommendations as tasks for resolution and assign to the correct resolver group or to the Service Management resolver group; and

(c) where a recommendation requires input from the Customer for reasons of cost, complexity or when considered a project task, raise a task for each recommendation. Service Management will discuss and agree with the Customer which of the recommendations should be progressed and follow the necessary process to allow recommendations to be implemented.

6.7 **Azure Workload Power Management**

6.7.1 Where the Company is providing Azure Workload Power Management, as identified on the Order Form, it will:

(a) maintain a schedule of workloads and times for power down/power up;

(b) execute automated power down and power ups at specified times;

(c) review the Azure Workload Power Management service monthly with the Customer; and

(d) resolve failures as Incidents in accordance with Specific Conditions X3 – Standard Operational Services

## 7 REPORTING

7.1 The Company will provide the following reports where the relevant Service is identified on the Order Form:

7.1.1 a Patch Management report, providing an overview of Patch Management in the relevant reporting period, including:

(a) status against most recent approved release;

(b) release % success; and

(c) devices below recommended currency;

7.1.2 an EDR Management report, providing an overview of EDR Management in the relevant reporting period, including:

(a) anti-virus compliance information; and

(b) security alerts;

7.1.3 a Backup Management Services report, providing an overview of the Backup Management Services in the relevant reporting period, including:

(a) total number of backups;

(b) successful backups performed; and

(c) failed backups.

7.1.4 a Storage Management report in accordance with paragraph 7.2

7.2 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.

7.3 All reports provided under this paragraph 7 will be distributed at the relevant frequency aligned to the relevant Service Management tier (as identified on the Order Form). Where no Service Management tier has been identified on the Order Form, the Company will not be obligated to provide any reporting identified in paragraph 7.

7.4 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.<br>**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.<br>**Alerts**: Highlight the alerts generated over the last 90 days and if there are any that are repeating themselves and need addressing.<br>**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.<br>**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.<br>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.<br>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. |

## 8 CUSTOMER OBLIGATIONS

8.1 The Customer will provide or otherwise comply with the following obligations set out in this paragraph 8.1, which are Customer Obligations for the purposes of this Contract:

8.1.1 unless otherwise provided by the Company under this Contract, remain responsible for all third party hardware, software, services and/or infrastructure that necessary to enable the provision of the Cloud Management Services;

8.1.2 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;

8.1.3 the Customer shall remain responsible for the security and firewalls of the Customer's communications links, equipment, software, services and processes unless agreed otherwise in writing with the Company;

8.1.4 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 the Customer will not unreasonably withhold or delay such approval;

8.1.5 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;

8.1.6 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;

8.1.7 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 unless such a server is specified to be provided by the Company;

8.1.8 either:

(a) allow for the set-up of a site to site VPN, or similar persistent connection as may be agreed in writing by 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 Cloud Management 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 by 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;

8.1.9 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;

8.1.10 ensure that that all Supported Equipment has 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 unless such Supported Equipment is classified as Legacy System Support;

8.1.11 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

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.

## 9 LEGACY SYSTEM SUPPORT

9.1 Where it is specified in the Order Form that the Company is providing Legacy System Support, the following non-exhaustive exclusions and/or limitations will apply in addition to any other exclusions and/or limitations set out in the Contract:

9.1.1 the Company will not apply Security Patches to the Legacy System unless otherwise agreed with the Customer. In the event that the Company does agree to apply a Security Patch to the Legacy System, the Customer acknowledges that such Security Patch may result in an Incident or render the Legacy System inoperable;

9.1.2 the Company will not be liable for any security breaches which are or are likely to be related to the Legacy System;

9.1.3 the Company will not apply Patch Management Services to the Legacy System, and the Company will not be responsible for resolving any related Incidents;

9.1.4 Enhanced Service Levels shall not apply to the Legacy System, however, the Company will respond to Incidents within the Incident Response Time;

9.1.5 the Company will use reasonable endeavours to resolve Incidents raised on a Legacy System, however, the Customer acknowledges that Incidents may be unresolvable and may render the Legacy System inoperable;

9.1.6 System Restores and/or System Rebuilds will not be available for Legacy Systems;

9.1.7 Legacy System Support cannot be provided to a Legacy System that has been migrated from one platform to another. The Company will only provide support on the platform in which the Legacy System was originally adopted into support;

9.1.8 the Company does not provide licences or licence key activation in relation to Legacy Systems;

9.1.9 peripheral software solutions which may work in the support or management of a Legacy System such as EDR, security, backup, monitoring and/or any other software used by the Company to provide the Cloud Management Services, may become unsupportable or inoperable should the Vendor make modifications to such peripheral software solutions or withdraw support for the Legacy System; and

9.1.10 where Supported Software reaches an End of Support Date during the Term the Cloud Management Services will be replaced by Legacy System Support.

## 10 EXCLUSIONS

10.1 The Company will have no liability (whether in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise) for any failure to provide the Cloud Management Services (including failing to meet any Service Level), or to pay any Service Credit (if applicable), to the extent caused by any interruption or failure of the Cloud Management Services arising directly or indirectly as a result of any of the following circumstances set out in this paragraph 10.1:

10.1.1 server maintenance or application maintenance carried out by the Customer or a third party;

10.1.2 any failure any act or omission of the third party cloud service provider and/or any other third party provider; and/or

10.1.3 as a result of any delay or failure by the Customer to provide or otherwise comply with the Customer Obligations;

and the Company reserves the right to levy additional charges on a time and materials basis in respect of such circumstances.

10.2 The Company does not guarantee the effectiveness of any EDR software. The Company is not responsible if the EDR software does not detect any specific Malicious Content and/or Cyber Threat.

10.3 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.

10.4 The following are not included in the Cloud Management Services:

10.4.1 requests for basic product training or technical consulting;

10.4.2 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 and/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 the Cloud Management Services through the introduction of Malicious Content, a Cyber Threat or any other form of cyber attack;

(d) any failure due to environmental conditions on-site;

(e) any failure due to loss of power to the Supported Equipment;

(f) any act or omission of Microsoft or any other Vendor;

10.4.3 any software other than the Supported Software and/or any programs or application used in conjunction with the Supported Software;

10.4.4 any management of third party break-fix maintenance providers. The Company will pass relevant information to the third party break-fix maintenance providers but the Company cannot manage those providers' responsibilities to meet the service levels offered to the Customer;

10.4.5 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;

10.4.6 management connectivity between the Supported Equipment and the Company; and/or

10.4.7 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.

10.5 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.

10.6 The Company reserves the right to refuse or withdraw Cloud 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 by the parties, the Company may continue to provide the Cloud Management Services on a reasonable endeavours basis.

## 11 SERVICE LEVELS

11.1 The Company will supply the Cloud Management Services in accordance with the applicable Service Levels set out in Specific Conditions document X3 – Standard Operational Services.

## 12 CHARGES

12.1 The Charges for the Cloud Management Services are as identified in the Order Form.

12.2 The Charges for the Cloud Management Services will be invoiced monthly in advance, with the first invoice issued by the Company on or around the Commencement Date.