SCHEDULE 4.4 – MANAGED SUPPORT SERVICES

1. APPLICATION

1.1 This Schedule which contains a description of the Managed Support Services form part of the for the provision of Services together with the **General Conditions**.

1.2 Definitions and interpretations that are specific to this schedule are set out in **Annex 1** and apply in addition to the definitions and interpretations set out in **Schedule 1 (Definitions)** of the **General Conditions**.

2 SERVICE DESCRIPTION

2.1 Where stated in the Order, the Supplier will provide the Customer with support services as described in this Schedule. Standard Support is detailed in **Part A** of this Schedule and Managed Support is detailed in **Part B** of this Schedule. Managed Service is detailed in **Part C** of this Schedule, and Managed Security as a Service ("**MSaaS**") is detailed in **Part D** of this Schedule.

INFRASTRUCTURE AUDIT

2.2 Where the Supplier deems it practicable to do so, it shall undertake an Audit of the Customer Network and/or the Supported Equipment to assess the Customer's requirements and to confirm the scope of Services and the associated charges prior to the Commencement Date.

2.3 Where an Audit under paragraph 2.2 has not been undertaken prior to the Commencement Date, the Charges shall be based solely on the information provided to the Supplier by the Customer and the Supplier shall undertake an Audit as soon as reasonably practicable thereafter.

2.4 If an Audit is undertaken after the Commencement Date and the Supplier discovers that the Customer's requirements are greater than those notified to the Supplier prior to the Commencement Date, or where the Supplier deems that the Customer Network and/or the Supported Equipment is in need of repair, the Supplier shall within thirty (30) days of an Audit notify the Customer of the revised scope and associated charges.

2.5 The Customer shall within five (5) Working Days of receipt of the revised scope and charges, notify the Supplier in writing of its:

2.5.1 acceptance of the revised scope and associated charges, which shall take immediate effect;

2.5.2 rejection of the revised scope and associated Charges, in which case the Customer shall continue to pay the original Charges and agrees and acknowledges that the Supplier shall continue to provide the Services in respect of the Customer's requirements as notified to the Supplier prior to the Commencement Date.

2.6 For the avoidance of doubt, if the Customer fails to notify the Supplier in accordance with paragraph 2.5 above, then the Customer shall be deemed to have accepted the revised scope and associated charges, which shall take immediate effect upon expiry of the notice period set out in paragraph 2.5 above.

3. CUSTOMER OBLIGATIONS

3.1 On and from the Commencement Date and throughout the Term, the Customer shall:

3.1.1 pay the Charges as and when they fall due;

3.1.2 make available all such facilities as the Supplier and the Supplier's Personnel reasonably require in providing the Services, including but not limited to:

(i) direct and remote access to the Customer Network and the Supported Equipment;

(ii) full and free access to the Site during the applicable Supported Hours; and

(iii) provide such reasonable assistance as the Supplier may request (e.g. providing sample output and other diagnostic information)

3.1.3 notify the Supplier immediately upon failure of any of the Customer Network and the Supported Equipment;

3.1.4 ensure that the Customer Network and the Supported Equipment is compliant with Applicable Law;

3.1.5 ensure that proper environmental conditions are maintained for the Customer Network and the Supported Equipment and shall maintain in good condition the accommodation of the Customer Network and the Supported Equipment, the cables and fittings associated therewith and the electricity supply thereto;

3.1.6 keep and operate the Customer Network and the Supported Equipment in a proper and prudent manner, in accordance with the manufacturer's operating instructions, and ensure that only competent trained employees (or persons under their supervision) are allowed to access the Customer Network and the Supported Equipment;

3.1.7 provide a secure, continuous power supply at the Site(s) for the operation of the Customer Network and Supported Equipment at such points with such connections at the Supplier specifies, and in order to mitigate any interruption to the Customer Network, its End Users and the Supported Equipment resulting from failure of the primary power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards;

3.1.8 ensure that all data held on the Customer Network and Supported Equipment is adequately backed up and keep full security copies of the Customer's programs, data bases and computer records and maintain a disaster recovery process;

3.1.9 be responsible for data cleaning, the integrity of any data provided to the Supplier and for all direct and indirect consequences of any errors in such data;

3.1.10 put in place and maintain up to date security measures to protect the Customer Network and Supported Equipment from viruses, harmful code, malicious damage and unauthorised direct and remote access to the Customer Network and Supported Equipment in accordance with Good Industry Practice;

3.1.11 save as set out in paragraph 3.1.13 below, not attempt to adjust, modify, configure, repair or maintain the Customer Network and/or Supported Equipment and shall not request, permit or authorise anyone other than the Supplier to carry out any adjustments, modifications, configurations, repairs or maintenance of the Customer Network and/or Supported Equipment;

3.1.12 ensure that the external surfaces of the Supported Equipment are kept clean and in good condition and shall carry out any minor maintenance recommended by the Supplier from time to time;

3.1.13 procure and maintain all relevant Licence Agreements and other licences and consents and, always comply with the terms of the relevant Licence Agreements and other licences and consents and all Applicable Law; and

3.1.14 inform the Supplier, in writing, of all health and safety rules and regulations and any other reasonable security requirements in place at the Customer Site(s), including any updates from time to time, and take all reasonable steps to protect the health and safety of the Supplier's Personnel whilst at the Customer's Site(s).

3.2 The Customer shall promptly implement recommendations by the Supplier in respect to remedial actions, whether prior to or following an Incident and confirms that it owns or will obtain valid Licence Agreements for all Software which are necessary to grant the Supplier access to and use of the Software for the purpose of fulfilling its obligations under this Schedule.

3.3 The Customer shall inform the Supplier of any changes to its applications, underlying Operating System and/or maintenance and support on services not provided by the Supplier, which may affect the validity of data obtained by the Supplier during an Audit.

3.4 The Supplier reserves the right, subject to providing the Customer with reasonable notice, to undertake a further Audit of the Customer Network and Supported Equipment, on an annual basis during the Term of this Agreement.

4 PART A STANDARD SUPPORT

4.1 The Supplier shall provide the Customer with the following;

4.1.1 access to Chess' PSA Platform;

4.1.2 contact details for the Service Desk;

4.1.3 provide Incident Management support in accordance with paragraphs 4.9 to 4.13 below;

4.1.4 use reasonable endeavours to remedy an Incident and in accordance with the relevant Service Level using remote support; and

4.1.5 subject to paragraphs 4.18 to 4.19, facilitate on behalf of the Customer, any claim made under a Third-Party Supplier warranty and/or support contract

hereinafter defined as **"Standard Support Services"**.

CHESS' PSA PLATFORM

4.2 The Supplier's service management system is essential to the provision of the Services and is designed to provide the Customer with important information about its account, systems and services.

4.3 Chess' PSA Platform enables the self-service management of the Services providing status updates and responses to assist in the monitoring and reporting of the Customer Network and Supported Equipment.

4.4 The Supplier shall provide to the Customer's designated administrator a unique login ID and password to access the Customer's account in Chess' PSA Platform. As a designated administrator, access to Chess' PSA Platform can be enabled for others, including control of areas and level of access, where required.

SERVICE DESK

4.5 The Service Desk provides a single point of contact for all Customer enquiries or queries raised by Chess' PSA Platform, email or telephone and the logging of all Incidents within the Supplier's service management system.

4.6 The Service Desk will provide support to the Customer during the Standard Support Hours, or where applicable, the relevant Support Hours as set out in the Order, where not specified the Standard Support Hours shall apply.

4.7 The Customer must when contacting the Service Desk provide, where available, details of the following:

4.7.1 contract number;

4.7.2 serial number or make and model;

4.7.3 details of Supported Equipment;

4.7.4 Customer contact information; and

4.7.5 full description of the problem including Software being used and any error messages.

SUPPORT HOURS

4.8 From the Commencement Date, the Supplier shall provide the Service(s) in accordance with the Support Hours selected by the Customer, subject to an additional charge, to extend the Standard Support Hours and as set out in the Order, as further described below:

	DAYS	HOURS	BANK HOLIDAYS
Standard Support	Mon – Fri	08:00 to 18:00 Hrs	Excluded
Advanced Support	Mon – Fri	07:00 to 19:00 Hrs	Excluded
Premium Support	Mon – Sun	24 Hrs	Included

INCIDENT MANAGEMENT

4.9 Where the Customer notifies the Supplier of an Incident in relation to the Customer Network and/or Supported Equipment, the Supplier shall log, process and manage Incidents through its Service Desk.

4.10 The Service Desk undertakes the following:

4.10.1 single point of contact for all requests;

4.10.2 escalation through 1st, 2nd and 3rd line support Engineer; and

4.10.3 Incident Management through to Resolution where possible;

4.10.4 remote Resolution of Incidents, where possible;

4.10.5 on Site Resolution of Incidents, where applicable; and

4.10.6 Third Party Supplier escalation, where applicable.

in accordance with the Incident Management process and applicable Service Levels, provided always that the Incident is not within any of the Excluded Events or is outside of the scope of the Services as further detailed in paragraph 5.34 below.

4.11 All Incident resolutions are verified with the Customer and/or its End Users in accordance with ITIL Methodology, before the Incident is deemed Resolved.

4.12 For all Incidents in relation to:

4.12.1 Excluded Events;

4.12.2 additional items not listed as Supported Equipment; or

4.12.3 where support is deemed outside of the scope of the Services

the Supplier shall use reasonable endeavours to respond to such Incidents, and the Customer shall be liable for time spent, costs and expenses incurred by the Supplier which shall be charged in accordance with its standard hourly rates and Tariffs.

4.13 Incidents referred to in paragraph 4.12 above shall not be counted or considered in relation to the performance of any Service Levels.

REMOTE SUPPORT

4.14 The Service Desk shall provide remote assistance using a non-invasive web and LAN based remote access toolkit reducing the requirement for local, desk side visits.

4.15 The Service Desk will aim to resolve Incidents at first line, where this is not possible, the Incident will be escalated to the appropriate 2nd / 3rd line subject matter expert in accordance with the Incident Management process.

4.16 Except where the Supplier deems necessary, attendance at Site of an Engineer is not included within the Standard Support Services.

4.17 If the Customer requests an Engineer to attend Site, this shall be subject to the Standard Schedule of Rates applicable at the time and will be charged separately on a time and materials basis.

THIRD PARTY WARRANTY SUPPORT

4.18 Where the Supported Equipment has a valid Third-Party Supplier warranty and/or support contract in place, the

Supplier shall facilitate on behalf of the Customer any claim made under the Third-Party Supplier warranty and/or support contract, in respect of an Incident identified and logged in accordance with this paragraph 4.

4.19 Where the Supported Equipment does not have a valid Third-Party Supplier warranty or support contract, or the Third Party Supplier no longer provides appropriate support, the Supplier shall use reasonable endeavours to respond to an Incident, and the Customer shall be liable for time spent, costs and expenses incurred by the Supplier which shall be charged in accordance with its standard hourly rates and Tariffs.

ESCALATION SUPPORT

4.20 The Supplier may at the option of the Customer, provide Escalation Support only to compliment the Customer's current support environment, which may include one of the following options:

4.20.1 1st Line Escalation Support – the Service Desk will perform the basic triage, identification and primary actions for any Incident and then escalate to either the Customer or a Third-Party Supplier, or;

4.20.2 3rd Line Escalation Support – the Customer shall remain responsible for all 1st line and 2nd line support and shall, where applicable escalate Incidents to the Supplier via its Service Desk to assist in the escalation of 3rd line support to a Third Party Supplier;

as further detailed in **Annex 3**.

INCIDENT BASED BILLING MODEL

4.21 Where stated in the Order, Standard Support will be provided by way of an Incident Based Billing Model whereby the Supplier will charge the Customer Incident Based Charges which are fixed Charges per Incident as per its Standard Schedule of Rates.

4.22 The Incident Based Billing Model is only available where the Supplier is providing System Monitoring and Patch Management Services as detailed in **Part B. T**he Recurring Charges for these Services will be billed annually in advance per Device pursuant to paragraph 10.2.2 in addition to the Incident Based Charges.

5 PART B – MANAGED SUPPORT

5.1 Where stated in the Order, the Supplier shall provide the Customer with the Standard Support Services as set out in **Part A** of this Schedule, together with one or more of the following options:

5.1.1 System Monitoring and Alerts;

5.1.2 Network Infrastructure Support;

5.1.3 End User Support;

5.1.4 Anti-Virus Support;

5.1.5 Patch Management;

5.1.6 Back Up Management;

5.1.7 Technical Attendance; and

5.1.8 Health Checks.

as further detailed in **Part B** of this Schedule and hereinafter defined as "**Managed Support Services**".

SYSTEM MONITORING AND ALERTS

5.2 The Supplier shall provide real-time monitoring with intelligent alerting, subject to the mandatory installation of the Supplier's preferred RMM Platform.

5.3 The Supported Equipment will be installed with RMM Agents to monitor and help manage the current state at any time, with data from the Customer Network being securely passed between the Supported Equipment and the RMM Platform and displayed for the Supplier to action or escalate as appropriate.

5.4 Each RMM Agent installed is responsible for monitoring the following details on the Customer Network and Supported Equipment as standard, as well as collecting performance data on the following metrics for reporting purposes:

5.4.1 Disc Space Performance – capacity, capacity forecasting, bottlenecking, disc read/write access;

5.4.2 CPU Performance – usage, forecasted usage, CPU leak, breach of threshold;

5.4.3 Memory Performance – breach of threshold, usage and forecasting, bottlenecking, paging and swap;

5.4.4 Event Log Management – application, security and system, and;

5.4.5 Operating System Monitoring – current status

5.5 The Supplier shall agree with the Customer criticality and business impact for the Customer Network and Supported Equipment, which will be stored within the RMM Platform for reference by the Service Desk, with required actions and escalation procedures based upon the agreed criteria also agreed and stored on the RMM Platform for reference.

5.6 Any changes or additions to the monitoring requirements shall be made by agreement between the Supplier and the Customer in accordance with the Change control process. A monitoring schedule change shall be undertaken within five (5) Working Days of the request.

NETWORK INFRASTRUCTURE SUPPORT

5.7 The Supplier shall, where applicable, provide the Customer with full Incident lifecycle support of the Customer Network and Supported Equipment which is used by the Customer to support its normal business operations, including one or more of the following options:

5.7.1 Hardware – maintain and deliver support in accordance with the Service Levels on applicable Supported Equipment, subject to a valid Third-Party Supplier warranty or support contract, and;

5.7.2 Operating System Software – maintain and deliver support in accordance with the Service Levels on applicable Operating System Software, subject to a valid License Agreement

where appropriate and as set out in the Order. The services set out in this paragraph 5.7 may be supplied alongside End User Support or as standalone service.

5.8 Support is focused on the active monitoring and care of the Customer Network and Supported Equipment on which the Customer and the End Users rely upon, through the RMM Platform (subject to the installation of RMM Agents) and is predominately delivered with remote support sessions by use of remote access tools, which enable the Supplier to monitor and alert on various metrics.

5.9 The Operating System Software currently supported by the Supplier are as follows:

5.9.1 Microsoft server operating systems within standard or extended support as further defined at https://support.microsoft.com/en-us/lifecycle/selectindex;

5.9.2 any systems deployed via the Supplier and with a valid Third-Party Supplier warranty;

5.9.3 any of the Supplier's products and services purchased by the Customer and as set out in the Order.

END USER SUPPORT

5.10 The Supplier shall, where applicable, provide support to the Customer focused on the End Users and their Devices which is tailored to provide resolutions to everyday Incidents and to enable End Users to access their Applications and Operating System including the following options:

5.10.1 Devices – maintain and deliver support in accordance with the Service Levels on applicable Devices, subject to a valid Third-Party Supplier warranty or support contract, and;

5.10.2 Application Software – provide troubleshooting support to identify accessibility or functional problems, with appropriate escalation, in accordance with the Service Levels on applicable Applications, subject to a valid Licence Agreement

where appropriate and as set out in the Order. The services set out in this paragraph 5.10 may be supplied alongside Network Infrastructure Support, Additional Services or as standalone service.

5.11 Support is focused on the active monitoring and care of the Devices on which the Customer and the End Users rely upon, through the RMM Platform (subject to the installation of RMM Agents) and is predominately delivered with remote support sessions by use of remote access tools, which enable the Supplier to monitor and alert on various metrics.

5.12 The Operating System supported by the Supplier as follows:

5.12.1 Microsoft windows desktop operating system within standard or extended support as further defined at https://support.microsoft.com/en-us/lifecycle/selectindex;

5.12.2 Apple Mac OS, current supported version from the Third-Party Supplier; or

5.12.3 other Operating Systems as further detailed in the relevant Order.

5.13 The following Applications (where installed upon the local Device and not streamed or cloud based), can be supported by the Supplier as follows:

5.13.1 Microsoft Office applications as stated in **Schedule 3.6(A) Microsoft Services**;

5.13.2 any applications deployed via the Supplier and with a valid Third-Party Supplier warranty;

5.13.3 any of the Supplier's products and services purchased by the Customer and as set out in the Order; and

5.13.4 any other applications may be supported on a reasonable endeavours' basis, subject to an additional charge.

ANTI-VIRUS SUPPORT

5.14 The Supplier shall, where specified in the Order, provide monitoring and support services for all Incidents relating to anti-virus Software provided by the Supplier or where prior agreement with the Supplier, the Customer's legacy anti-virus software, as set out in the applicable Order.

5.15 The Supplier requires remote monitoring and access to the anti-virus software installed on the Customer Network and Supported Equipment through its RMM Platform to ensure that the anti-virus software definition files are updated on a regular basis as required.

5.16 The Supplier shall maintain and deliver support in accordance with paragraph 5.14 above and the Service Levels, with Incidents being managed through the Service Desk with anti-virus software configured to automatically update definition files. Updates to the anti-virus software is excluded and all updates shall be subject to a Change Request.

PATCH MANAGEMENT

5.17 The Supplier offers an automated patch management service as well as scoped patch management services. The automated patch management service is outlined at paragraphs 5.18 to 5.24 below. Where the Supplier provides a scoped patch management service, that service shall be detailed in the Order where it forms part of the Managed Support Service. Ad-hoc bespoke patch management services may also be provided upon request and will be provided as Professional Services and shall be subject to an agreed SOW and **Schedule 4.2 (Professional Services**).

5.18 The Supplier's remote patch management service provides comprehensive proactive service across the Customer Network and Supported Equipment using its RMM Platform, which provides real time monitoring of Customer Network and Supported Equipment to ensure that applicable patches/updates are being used.

5.19 Hardware drivers, firmware and associated management Software updates are outside of the scope of patch management services. The Supplier recommends that updates are applied to keep the Customer Network within Third Party Supplier's supported versions, and the Customer can request the Supplier to undertake an infrastructure health check at any time, subject to an additional charge to the Customer.

5.20 Before any patches or updates can be applied to servers, they must have the relevant recovery procedures in place, including but not limited to a full or adequate back up of the data and Operating System. Once the server is updated, testing procedures will be carried out to validate the system, and applications have not been adversely affected.

5.21 The Customer is responsible for ensuring the backup is in place and viable with respect to automatic patching and will report any failures to the Supplier so the effected patching schedules can be adjusted.

5.22 Emergency patches are subject to a Change Request and changes will be raised as and when either the Customer or the Supplier is made aware of the specific patch.

5.23 In the event of an error, the Supplier shall remove or roll back the patch identified as causing the problem and snapshots may be used by the Supplier to facilitate the removal but only in instances deemed necessary by the Supplier.

5.24 The Supplier shall support the Operating Systems and Third-Party Supplier Software listed in the Advance Software Management application catalogue which can be found at Advanced Software Management application catalog. The Supplier reserves the right to amend the catalogue from time to time. The Supplier shall only support the products listed in the catalogue unless otherwise set forth on the relevant Order.

BACK UP SERVICES

5.25 The Supplier shall provide remote management, using its RMM Platform, of the Customer's on-premises, or cloud- based solution, identifying issues, remote resolution or escalation to the Customer if an Engineer is required to attend Site.

5.26 The Supplier shall configure the RMM Platform to monitor the Customer's back-up solution and alert the Service Desk to any anomalies, so they can be investigated and resolved as follows:

5.26.1 respond to alerts generated (e.g. failed, incomplete, non-started or crashed tasks);

5.26.2 resolve, remotely alert (if possible) and restart the task to maintain the integrity of the data;

5.26.3 escalate to the Customer, via email, if the back-up task fails and cannot be resolved remotely;

5.26.4 modify tasks to remove file types that should not be selected (e.g. temp files, MDF, LDF etc);

5.26.5 produce a data protection report showing the back-ups over the month; and

5.26.6 provide a report from the RMM Platform detailing the number of alerts generated.

5.27 The back-up report can be generated monthly and is available to the Customer in Chess' PSA Platform, which consists of a single document which contains a list of back-up tasks, per server, detailing success or failure.

5.28 Where the Supplier has agreed, to transfer, duplicate or reinstall data or information as part of the Services, these services shall be subject to a separate Order.

5.29 The Supplier shall not be liable for any loss or corruption of data, as the Customer agrees that it is its own responsibility to back up all data and material on relevant storage media on a regular basis in accordance with Good Industry Practice, and it is a condition of the Supplier providing the Services that the Customer complies with the terms of this paragraph 5.29.

5.30 The Customer's sole and exclusive remedy for any loss or corruption of data shall be for the Supplier to use reasonable endeavours to restore such data or information to the most recent, uncorrupted copy of such data which the Supplier holds.

TECHNICAL ATTENDANCE

5.31 The Customer shall also have the option to purchase in advance, Technical Attendance Day(s), where the Supplier will provide remote support or attendance to Site of an Engineer to carry out Elective Changes as an addition to the Managed Support Services.

5.32 For the avoidance of doubt, Technical Attendance Days are not applicable for Customised Changes, which will be carried out, at the Customer's request, as Professional Services.

HEALTH CHECKS

5.33 Where the Supplier provides a health check service as part of the Managed Support Services, the health check service shall be detailed in the Order. Ad-hoc health check services can also be provided upon request and will be provided as Professional Services and shall be subject to an agreed SOW and **Schedule**

4.2 (Professional Services).

EXCLUSIONS

5.34 The Managed Support Services and the associated Charges shall not include the following:

5.34.1 systems engineering services, programming, reprogramming or reconfiguration of the Supported Equipment and operating procedures to provide improved or modified services or facilities;

5.34.2 development, modification or correction of any Software used in connection with the Supported Equipment or provision of the Managed Support Services;

5.34.3 recovery or reconstructions of any data or programs lost or corrupted as a result of any defect in the Supported Equipment;

5.34.4 electrical work external to the Supported Equipment or the support of accessories, ancillary items, including but not limited to, cabinets, infrastructure cabling or other devices not identified in the applicable Order;

5.34.5 any Supported Equipment which the Supplier reasonably considers to be end of life or Beyond Repair or for which consumables, spare parts, drivers or updates are not readily available or require essential maintenance not included in the Services;

5.34.6 defects in design, manufacture, installation or performance of Supported Equipment (except in relation to defects in installation, where the Supplier has carried out installation of the Supported Equipment);

5.34.7 supply of consumables and/or spare parts unless otherwise agreed in writing by the Supplier;

5.34.8 maintenance or repair of any power supply (including without limitation, any battery back-up and/or uninterrupted power supply) to the Supported Equipment; and

5.34.9 all Change Requests as further detailed in paragraph 9 below.

5.35 If the Supplier does agree to undertake any of the services set out in paragraph 5.34 above, the Supplier shall charge the Customer for providing such services, which shall be calculated in accordance with the Supplier's Standard Schedule of Rates, applicable at the time, together with any replacement parts and other costs and expenses reasonably incurred. Such services shall not be counted or considered in relation to performance of any Service Levels.

6 PART C – MANAGED SERVICES

6.1 Where stated in the Order, the Supplier shall provide the Customer with the Standard Support Services and Managed Support Services as set out in **Part A** and **Part B** above, together with the following:

6.1.1 Configuration and Optimisation;

6.1.2 Strategic Planning; and

hereinafter defined as **"Managed Services"**.

6.2 For the avoidance of doubt, the Managed Services shall only be provided where the Customer has taken all services as set out in **Part A** and **Part B** of this Schedule, without exception and has given the Supplier exclusive access to the Customer Network and Supported Equipment.

CONFIGURATION AND OPTIMISATION

6.3 The Supplier shall provide six (6) Technical Attendance Days per Contract Year, which is included in the Recurring Charges for the Managed Services, which may be utilised for one or more of the following tasks:

6.3.1 Configuration Management – reactive and proactive configuration and technical support of the Customer Network and Supported Equipment to ensure that the Customer Network and/or the Cloud Services works efficiently; and

6.3.2 Efficiency Optimisation – monitoring of the Customer's use of the Customer Network and/or the Cloud Services to identify efficiencies that could be made to the Customer Network and/or Cloud Services.

STRATEGIC PLANNING

6.4 The Supplier shall provide two (2) Working Days per Contract Year of Professional Services, which is included in the Recurring Charges for the Managed Services, which may be used for technical advice and design development, in accordance with **Schedule 4.2 (Professional Services)**.

6.5 Any further technical support services required outside of those included in the Recurring Charges for the Managed Services as set out above, shall be subject to the advance purchase of Technical Attendance Days in accordance with paragraphs 5.31 to 5.32 above and/or **Schedule 4.2 (Professional Services)**.

7 PART D – MANAGED SECURITY AS A SERVICE ("MSaaS")

7.1 Where stated on the Order, the Supplier will provide the Customer with MSaaS. MSaaS provides customers with an enhanced security layer delivered through advanced endpoint protection, threat detection, response capabilities, email security, user awareness training, cloud security telemetry, and data protection services.

7.2 MSaaS is only available to Customers who have Standard and Managed Support Services with the Supplier as detailed in **Part A and B** of this Schedule. MSaaS is not available to Customers who have Standard Support on an Incident Based Billing Model even if Managed Support or Managed Services are also being provided.

7.3 MSaaS includes all service components detailed in this paragraph 7. The Customer may choose to activate all or only some service components. The Customers requirements shall be detailed in the SOW and agreed with the Customer as part of the service onboarding process.

7.4 To provide this service, the Supplier requires the installation of the RMM Platform to monitor, manage and secure all endpoints which are agreed with the Customer as part of the onboarding process.

7.5 The Supplier will remotely monitor, manage and support Customer endpoints using ransomware detection monitors for the existence of cryptographic ransomware on endpoints using behavioural analysis of files and alerts. The Supplier will isolate any device to prevent the ransomware from spreading when detected.

SERVICE COMPONENTS

Anti-Virus

7.6 The Supplier shall implement and maintain enterprise-grade antivirus protection across all supported endpoints stated in the Agreement. This component is intended to safeguard systems against common malware and viruses through real-time scanning, heuristic analysis, and signature-based detection. The Customer acknowledges that antivirus technology, while effective against known threats, may not provide comprehensive protection against sophisticated or emerging attack vectors.

Endpoint Detection and Response (EDR)

7.7 The Supplier shall deploy EDR technology to deliver advanced threat detection and remediation capabilities. EDR is designed to identify and respond to complex cyber-attacks, including zero-day exploits and advanced persistent threats (APTs), which may evade traditional antivirus solutions. EDR functionality includes continuous telemetry collection, forensic analysis, and automated or manual response actions as deemed necessary by the Supplier.

Ransomware Detection

7.8 The Supplier shall implement ransomware detection measures to add an additional layer of security. This component is specifically designed to identify behaviours indicative of ransomware activity, including unauthorized encryption processes. Upon detection, the Supplier shall initiate mitigation protocols, which may include isolating the affected endpoint, terminating malicious processes, and notifying the Customer in accordance with the Service Levels.

Managed Detection and Response (MDR)

7.9 MDR is powered by the Rocketcyber Platform. This component is designed to deliver continuous, human-led monitoring and advanced threat analysis through a SOC. MDR functionality includes proactive threat hunting, identification of Indicators of Compromise (IOCs), and classification of security events as benign, suspicious, or malicious.

7.10 Upon confirmation of a critical threat, the Supplier, in conjunction with the SOC, shall initiate containment measures, which may include isolating the affected endpoint from the network to prevent lateral movement and further compromise. The SOC shall provide detailed incident triage, escalation, and remediation guidance and who will execute corrective actions in accordance with the Service Level detailed in the Incident Report SOC Document. The parties will comply with their respective obligations as per the Incident Report SOC Document. The Customer acknowledges that MDR services are intended to enhance detection and response capabilities but do not constitute a guarantee against all forms of cyber threats.

7.11 Rocketcyber's SOC works on behalf of the Supplier to detect, respond and remediate critical cybersecurity incidents via all tools and methods available to it.

7.12 Rocketcyber's incident response model is based on the NIST Framework for improving critical infrastructure cybersecurity and the MITRE ATT&CK Framework amongst others.

7.13 The Rocketcbver SOC will provide seamless log monitoring. It will monitor, search, alert and report on the network, cloud and endpoint log data spanning Windows, macOS, firewalls and network devices, Microsoft 365 and Entra ID.

7.14 The Rocketcyber SOC also provides real-time threat intelligence monitoring by connecting premium intelligence feed partners providing the Customer with a global repository of threat indicators for SOC analysts to hunt down attackers.

Email Security

7.15 The Supplier will:

7.15.1 supply software for filtering of phishing, spoofing, and malicious email content powered by Inky, a Kaseya company;

7.15.2 will provide real time scanning of inbound messages and provide URL rewriting/safe link protection and attachment sandboxing using the software; and

7.15.3 create and action proactive tickets for compromised accounts.

Phishing Simulation

7.16 The Supplier will provide 1 phishing simulation per quarter, pre-programmed for 12 months. Scheduled during onboarding with Customer approval powered by Bullphish ID, a Kaseya tool. The Supplier will provide customer access to the Bullphish ID software platform for security awareness training modules for users. The Supplier will offer scoring and behaviour analysis driven by simulation performance. Delivered via a quarterly user risk report with trends and repeat-offender identification.

Dark Web Monitoring

7.17 The Supplier will provide monitoring of the Customer's domain for compromised credentials, personal data, or exposed information powered by Darkweb ID, a Kaseya tool. The Supplier will:

7.17.1 complete a retrieval of breach intelligence including passwords, PII, and login data and present Initial baseline report at onboarding;

7.17.2 create and action tickets for rapid alerts for critical findings; and

7.17.3 provide a monthly report summarising newly discovered exposures.

SaaS back-up for M365 cloud Apps

7.18 The Supplier will:

7.18.1 provide automated backups of Microsoft 365 - emails, files, and collaboration data; and

7.18.2 provide a restore capability for accidental deletion, corruption or security incidents.

7.19 The Customer acknowledges and agrees that the Supplier will automatically provision a License for the SaaS Protection Service for every new Microsoft User which is added to the Customer's Microsoft account. Where a license for the SaaS Protection Service is automatically provisioned, the license(s) shall be coterminous with the Minimum Term of the licenses provided in the initial Order placed by the Customer for the SaaS Protection Service. All licenses for the SaaS Protection Service will therefore expire on the same date.

7.20 If the Customer does not wish for a license to be automatically provisioned for an additional User in accordance with paragraph 7.19 above, then it must notify the Supplier in advance of the User being added to the Customer's Microsoft account.

7.21 The Customer acknowledges and agrees that where a User is removed from the Customer's Microsoft account, the relevant license for the SaaS Protection Service will not automatically be removed or terminated but rather it will continue to be provided unless and until the relevant license is terminated by the Customer in accordance with the terms of the Agreement.

7.22 If a Backed-Up Site amends its API guidelines in such a way that materially affects the Supplier's or Kaseya's ability to access the Backed-Up Site to provide the SaaS Protection Service in accordance with the Specifications, and if the Supplier and Kaseya is unable to perform substantially the same functionality, either party may terminate the applicable Order by providing to the other thirty (30) days' written notice.

SERVICE LEVELS

7.23 The Supplier shall use reasonable endeavours to meet the Service Levels detailed in **Annex 2** of this Schedule in relation to all Service Components save for MDR. For MDR Specific Severity Levels for Incidents, the Service Levels detailed in the Incident Report SOC Document shall apply.

KASEYA LICENSE TERMS

7.24 The Customer acknowledges and accepts the terms of the applicable Kaseya Product Terms (as amended by Kaseya from time to time) are incorporated and form part of this Agreement. The terms applicable to each Service component are referred within the Definitions at **Annex 1** of this Schedule. Where the Customer is granted access or rights to use the service components directly, the Customer agrees to use the services in accordance with the Kaseya Product Terms.

7.25 Subject to the terms of this Agreement, applicable Product Terms, the Supplier grants to the Customer during the Minimum Term (and any Successive Term) a non-sublicensable, non-exclusive, revocable, nontransferable right to use the Kaseya Products (a "License") for use as part of the Services as described in this Schedule only.

7.26 Except for the limited rights granted in this Schedule, Kaseya retains all rights, title, interest and Intellectual Property Rights in the Services, portals, materials and documentation.

7.27 The Customer is responsible for the security of all the Customer's access credentials relating to the Kaseya Services including any action the Customer permits any person or entity to take related to the SaaS Protection Service and Backed-Up Data using the Customer's access credentials.

7.28 The Customer is responsible for the proper configuration and maintenance of safeguards as they relate to access to and use of the Kaseya Services and Backed-Up Data, including but not limited to individual Administrator and User permissions, local Device access, network connectivity and internet connectivity.

7.29 The Customer agrees to notify the Supplier as soon as practicable of any unauthorised use of any access credentials, password or account or any other known or suspected breach of security.

Restrictions

7.30 The Customer and End Users may not, nor permit, facilitate or authorise any third party to:

7.30.1 use the Services other than as permitted under this Schedule;

7.30.2 remove or destroy any copyright or other proprietary markings contained in or on any Services or its Specifications;

7.30.3 access or use the Services in any manner that could damage, disable, or overburden or otherwise interfere with or disrupt the Services, any networks or security systems;

7.30.4 reverse engineer, decompile, disassemble, or otherwise attempt to extract source code from the Services, except to the extent this restriction is expressly prohibited by Applicable Law;

7.30.5 copy, modify or create derivative works of the Services;

7.30.6 develop license keys or codes other than those provided by Kaseya or the Supplier or attempt to alter, defeat, or circumvent access restrictions or any other disabling mechanism which may reside within the Services;

7.30.7 assign, sublicense, rent, timeshare, loan, pledge, lease, or otherwise transfer the Services, or directly or indirectly permit any unauthorized third party to use or copy the Services;

7.30.8 conduct or disclose the results of any form of benchmarking, pen testing or competitive analysis of the Services;

7.30.9 extract portions of any software or firmware for use in other applications;

7.30.10 register or remotely monitor the Services through any management portal other than the portals provided by Kaseya or the Supplier; or

7.30.11 access any Service for the purposes of competing with Kaseya or the Supplier, using a false identity or false information, for reasons other than a good faith desire to use the Services or otherwise to (i) build a competitive product or service; (ii) copy any, or build a product using, ideas, features or graphics sourced from the Services.

Limitations On Services / Content

7.31 The Services and Backed-Up Data may not;

7.31.1 be used to send any unsolicited commercial email or invitation in violation of Applicable Law;

7.31.2 be used to request, collect, store, transmit, process or disclose any unencrypted personally identifiable data (such as payment card numbers or social security numbers) in violation of any Applicable Law; be deceptive, fraudulent, harmful, abusive, harassing, threatening, indecent, obscene, racially, ethnically, or otherwise objectionable, hateful, tortious, libellous, defamatory, slanderous, or otherwise in violation of Applicable Law;

7.31.3 infringe or misappropriate any Intellectual Property Rights or other rights of any third party;

7.31.4 be used in a manner which constitutes or encourages conduct in breach of Applicable Law;

7.31.5 contain or be used to transmit or otherwise make available any viruses or similar malicious software that may damage the operation of any computer, network, system or the Services;

7.31.6 violate the Kaseya Product Terms or any other license agreement or agreement which the End User of Content is subject to;

7.31.7 be used in jurisdictions where the Services is not certified for use or where use is not allowed by Applicable Law; or

7.31.8 be used to send materials to individuals under the age of majority in his or her place of residence ("**Minors**"), or to harm Minors in any way, or that would subject us to any Applicable Law governing children's privacy or otherwise related to protecting Minors.

7.32 If the Supplier reasonably believe the Service use or Backed-Up Data:

7.32.1 violates any of the restrictions in the foregoing paragraphs;

7.32.2 may disrupt or threaten the operation or security of any computer, network, system or the Services; or

7.32.3 may otherwise subject the Supplier to liability

the Supplier reserves the right to refuse or disable access to the Services and/or Backed-Up Data. The Supplier may also take such action as required to comply with Applicable Law. The Supplier will use reasonable efforts to contact the Customer prior to taking such action. However, the Supplier may restrict access to the Services or Backed-Up Data without prior notice as necessary to comply with Applicable Law or to protect against damage or security threats. If the Supplier takes any such action without prior notice, the Supplier will later provide notice to the Customer, unless prohibited by Applicable Law.

7.33 Use of the Services is not authorized, will not be supported by us, and any warranties will be void, if the Services are modified in any way or used in a manner for which they are not intended, including but not limited to (i) integrating or combining with software or hardware that is not recommended or approved; (ii) installing a different operating system (OS) on a hardware Device; (iii) using a backup Product in a prolonged virtualized production environment instead of as a backup application (except for a limited testing period or in the event of a documented business continuity event); (iv) use in jurisdictions where the Service is not certified for use, or where use otherwise breaches Applicable Law; or (iv) use, access or support of any Service by unauthorized personnel or by those who are not knowledgeable and competent with respect to the Service.

Trial Use

7.34 If a Service is being used during a trial or evaluation, this Agreement and the applicable **Kaseya Product Terms** (except, typically, for the payment obligation) will apply to such authorized evaluation or trial period. The Supplier reserves the right to terminate any evaluation or trial use of the Product at any time at its sole discretion.

Open-Source Software

7.35 If a Service contains open-source software, those pieces of open-source software are licensed under the open-source license terms as chosen by the provider of the applicable open-source software. Such open-source license terms can be found in either the open source_licenses.txt file accompanying the applicable Service or the Documentation. Open-source license terms may contain additional rights benefiting you and will take precedence over any other agreement between you and Kaseya with respect to the applicable open-source software. If the license for open-source software requires Kaseya to make the open-source software available to you without charge, you may a copy by contacting the Supplier.

Service Conditions

7.36 The Customer may be required by the Supplier and/or Kaseya to install certain Software to use the Kaseya Services, if so, the following terms apply:

7.36.1 the Customer may install and use the Software only for use with the Kaseya Services;

7.36.2 the **Product Terms** may limit the number of copies of the Software the Customer may use or the number of Licensed Devices on which the Customer may use it;

7.36.3 the Customer's Use Rights begin when the Kaseya Service are activated and ends when the Customer's Use Rights for the Kaseya Services ends;

7.36.4 the Customer must uninstall the Software when the Customer's Use Rights ends; and

7.36.5 the Supplier and/or Kaseya may disable the Kaseya Services at any time.

7.37 Products may be programmed to track the number of deployed License Units (such as seats, authorized devices, or users). The Customer hereby consents to such tracking and shall not, directly or indirectly, circumvent, impede or obstruct such tracking or reporting. You grant the Supplier and Kaseya the right to track and monitor use by all End-Users and you will provide access to your records, personnel and representatives, during your normal business hours to verify compliance with this Agreement, including such License limits. If an audit reveals that Licenses used by you exceeded the amounts paid for and that additional amounts are owed, you shall pay such amounts immediately. The Supplier will bear the cost of the audit unless the audit reveals that the additional amounts owed are in excess of five percent (5%) of the total License Fees paid during the audited time period, in which case the reasonable cost of the audit shall be paid by the Customer.

7.38 The Customer agrees that Kaseya and/or the Supplier may, and you hereby authorise, us at any time and from time to time, to interact remotely with the deployed Services in order to test, troubleshoot, support or update such Service, or to analyse use or modify the Services or the environment in which it operates.

7.39 Kaseya reserves the right at any time to make Enhancements to, replace, modify, discontinue or add to the Services, including revisions to Specifications, features and functionality. The Supplier will use reasonable commercial efforts to provide the Customer notice of any material consequential changes to the Services being provided by updating relevant information in the applicable Online Portal.

7.40 The Customer may only obtain updates or upgrades for the Software from the Supplier or Kaseya and Kaseya may recommend or download to Licensed Devices updates or supplements to the Software, with or without notice to the Customer.

7.41 Where Kaseya introduces features, supplements or related software that are new (i.e. that were not previously included with the Subscription), Kaseya may provide terms or make updates to the Kaseya Product Terms that apply to the Customer's use of those new features, supplements and related software.

7.42 The Supplier and Kaseya may provide the Customer with information and notices about the Kaseya Services electronically, including via email, through the portal for the Kaseya Services, or through a web site that the Supplier or Kaseya identifies.

7.43 The Software may contain third party software components and unless otherwise disclosed in that software, Kaseya, not the third party, licences these components to the Customer under Kaseya's licence terms and notices.

7.44 In the event we reasonably believe any Service use, configuration of Service or Content: (i) violates any of the restrictions in the foregoing sections; (ii) may disrupt or threaten the operation or security of any Service, data, Content, computer, network, or system of yours, Kaseya's, or any third party; or (iii) may otherwise subject us or a third-party to liability or damage, we reserve the right to suspend services or disable access to the Service, Portal, platform or Content. We may also take such action as required to comply with Applicable Law. We will use reasonable efforts to contact you prior to taking such action. Notwithstanding the foregoing, we may suspend a Service or restrict access to Service or Content without prior notice in an emergency or as necessary to comply with Applicable Law or protect against liability or damage as described herein. Kaseya and the Supplier shall have no liability to you as a result of suspension or termination under this section.

7.45 The Customer agrees to immediately notify the Supplier of any unauthorized use, copying, or disclosure of the Service or Content of which you become aware, as well as any use of Service in a manner that is contrary to Applicable Law, including use of Service in areas where it is not certified for use or that violate export laws. The Customer agrees to immediately take such actions as are necessary to end and prevent any such use, copying, or disclosure. The Customer acknowledges and agrees that any breach of this paragraph may cause immediate and irreparable injury to the Supplier, Kaseya or to third parties, and in such event, the Supplier may immediately suspend or terminate access or use of a Service without notice and without liability to you or any third party, and to seek and obtain injunctive relief, without bond or other security, in addition to other remedies available at law and in equity.

7.46 The Customer agrees to (i) use reasonable efforts to prevent and terminate any unauthorized access to, or use of, your Portal Accounts or any access credentials to your Portal Accounts; and (ii) notify the Supplier immediately of any known or suspected unauthorized access to, or use of, your Portal Accounts or any access credentials to your Portal Accounts. The Supplier and Kaseya will not be liable for any loss incurred as a result of any unauthorized access to, or use of, your Portal Accounts or any access credentials to your Portal Accounts. The Supplier and Kaseya reserve the right to change, suspend, remove, disable or impose access restrictions on any access credentials to your Portal Accounts at any time without notice to you if Kaseya believes such actions are needed to avoid actual or potential damage to you, Kaseya or any third party. The Customer agrees to cooperate with the Supplier and/or Kaseya by providing any information that is reasonably requested by or on behalf of Kaseya to investigate and resolve any unauthorized access to, or use of, your Portal Accounts or any access credentials to your Portal Accounts, or any other compromise involving your Portal Account(s).

Customer Data And Information

7.47 Following termination of the Agreement and/or the Services the Customer the Supplier and Kaseya reserve the right to permanently delete all related Content including the Customer Data or disable access to such Content and Customer Data immediately and neither the Supplier nor Kaseya shall be liable for such actions.

7.48 Under no circumstances shall the Supplier be liable for any loss or damage to Customer Data. The Customer accepts the responsibility for backing up Customer Data and shall ensure that the Customer's processes in this respect are adequate.

Backed Up Data

7.49 The SaaS Protection Service may be configured to designate the geographic region where Backed-Up Data associated with the SaaS Protection Service is stored. Kaseya's Data Processing Addendum is incorporated into this Schedule where the SaaS Protection Service is configured to store Backed-Up Data in the European Economic Area.

7.50 The Customer represents and warrants it has all rights (including from Backed-Up Sites and Users) as necessary to permit access, copying and use of Backed-Up Data with the SaaS Protection Service.

7.51 The Customer is responsible for the accuracy, quality and legality of the Backed-Up Data, and the means by which the Customer acquired rights to the Backed-Up Data for use with the SaaS Protection Service. For purposes of this Schedule, Backed-Up Data is the property of Customer, not any User, and the Supplier is under no obligation to inform Users that the Customer controls such information with the Supplier.

7.52 The Customer, for itself and its Users, authorises the Supplier and Kaseya to access and interact with the Backed-Up Site to retrieve Backed-Up Data and grants the Supplier and its Kaseya a limited, royalty-free, non-exclusive, assignable license to use, copy, reformat, display, disclose and distribute the Backed-Up Data solely for providing the SaaS Protection Service as described in this Schedule, including as authorised by an Administrator for support, and as described in the Kaseya's Privacy Policy.

7.53 The Customer retains all its right, title and interest in and to the Backed-Up Data, and the Supplier and Kaseya neither own nor acquire rights in the Backed-Up Data other than the rights expressly granted under this Schedule.

7.54 The Supplier and Kaseya will use physical, technical and administrative safeguards, consistent with commercially reasonable industry practices, designed to secure the confidentiality, integrity and availability of Backed Up Data under its control against accidental or unauthorized loss, access or disclosure.

7.55 The Supplier and Kaseya will use the same safeguards for all Backed-Up Data, regardless of its nature or contents. The Supplier and Kaseya are both a Processor and not a Controller of all Backed-Up Data.

7.56 The Customer must maintain authorisation and access to the Backed-Up Sites so that the Supplier and Kaseya are regularly able to access Backed-Up Data for purposes of providing the SaaS Protection Service.

7.57 The Customer agrees and acknowledges that Backed-Up Data may not be available or restorable;

7.58 if the Customer changes such access authority or otherwise restricts the Supplier's and/or Kaseya's access to such Backed-Up Site;

7.59 due to unavailability of the Backed-Up Site; or

7.60 with respect to modifications to the Backed-Up Data that are not captured in the backup frequency or retention schedule for the SaaS Protection Service.

7.61 Unless otherwise agreed to in writing by the Supplier, the Customer agrees that Backed-up Data will not contain Special

Category Data. If the Backed-Up Data does include Special Category Data, the Customer shall indemnify the Supplier for all losses, damages, costs, expenses or other liabilities incurred by, awarded against or agreed to be paid by the Supplier arising from, or in connection with the Processing of the Special Category Data. The Customer further acknowledges that the limitation of liability provisions contained in this Schedule and the **General Conditions** shall not apply to the indemnity in this paragraph 7 and as such the Customer's liability to the Supplier shall be unlimited.

Other Information and Data

7.62 The Customer hereby represents and warrants that: (i) it has sufficient rights and all required third-party consents, permissions or licenses in and to the Content as may be necessary and appropriate for use of the Content with the Product; (ii) it authorize us to access and interact with the Services to retrieve and process Content; and (iii) it grants Kaseya a limited, worldwide, royalty-free, non-exclusive, assignable license to copy, host, record, view, reformat, disclose, transmit, display and otherwise use the Content as necessary or desired, in each case solely for the purposes of providing the Services and as otherwise necessary for Kaseya and the Supplier to fulfil its obligations and exercise its rights under this Agreement including applicable Product Terms and Orders. The Customer is responsible for the collection, accuracy, quality, completeness and legality of the Content and the means by which the End-User acquired rights to the Content for use with the Services, and the Supplier and Kaseya will not be responsible or liable for the unauthorized access to, alteration of, or deletion, correction, destruction, corruption, damage, loss or failure to secure or store Customer Content. The Customer bears sole responsibility for adequately controlling, processing, storing and backing up Customer Content.

7.63 Except for the limited license granted hereunder, the Customer retain all existing rights in and to Content. Kaseya and the Supplier will use and process the Content as necessary to provide and support the Services and will not otherwise access Content other than as permitted under this Agreement, the applicable Terms of Use, as or as authorized by you for support. If you authorize an End-user to directly use or support a Service, including any features designed to be accessible to your End-User, as between the Customer, the Supplier and Kaseya, the Customer is responsible for all such access and use by the End-User.

7.64 Services may be configured to designate the geographic region where Content associated with a Product is stored. Kaseya complies with the EU-US Data Privacy Framework (EU-US DPF) and the UK Extension to the EU-US DPF, as well as the Swiss-US Data Privacy Framework (Swiss-US DPF). Kaseya has certified to the U.S. Department of Commerce that it adheres to the EU-US Data Privacy Framework Principles regarding the processing of personal data received from the European Union and the United Kingdom and certified to the Swiss-US Data Privacy Framework Principles with regard to the processing of personal data received from Switzerland. (collectively, the "Privacy Framework Principles"). In addition, the Kaseya standard European, Swiss and/or UK Data Processing Addendum(s) (each a "Kaseya DPA") are incorporated into this Agreement if a Product is configured to store Content in the European Economic Area, the United Kingdom, Switzerland. If a Product is configured to store content in the United States and is used to process personal information of California consumers under the California Consumer Privacy Act of 2018, as amended, and the final regulations thereunder (collectively the "CCPA"), Kaseya will comply with the CCPA and we are a "service provider" with respect to the personal information of California consumers we process. We will not sell such personal information and will not retain, use or disclose such personal information for any purpose other than for the purpose described in this Agreement, the applicable Product Terms of Use, or as otherwise permitted by the CCPA or applicable law. More information about how Kaseya processes personal information can be found in our Privacy Statement, accessible by clicking here. If there is a conflict between this Agreement and our Privacy Statement, the Privacy Statement shall govern. If there is a conflict between this Agreement and a Kaseya DPA, the Kaseya DPA shall govern. In all cases, and despite any conflict with any Kaseya agreement or statement, the Privacy Framework Principles shall govern.

7.65 Kaseya uses physical, technical and administrative safeguards designed to help secure the Services and Content under our control against accidental or unauthorized loss, access or disclosure. However, no system of data transmission, storage or retrieval can be made entirely impenetrable and despite the measures employed, the Services and Content are not guaranteed against all security threats or other vulnerabilities, and the Customer acknowledges that it uses the Services with all Content at its own risk. Notwithstanding anything to the contrary in this Agreement, Kaseya's security measures extend only to those systems, networks, network devices, facilities and information technology components over which Kaseya has control. The are responsible for the proper configuration and maintenance of physical, administrative and technical safeguards as they relate to access and use of the Services, accounts and Content. In no event will Kaseya or the Supplier be responsible, nor will we have any liability, for physical, administrative, or technical controls related to the Services or Content (including without limitation Personal Information) that the Customer controls, including but not limited to access credentials (including passwords), network connectivity and internet connectivity. The Customer agree to (i) change your passwords and other access credentials to Services and Portal Accounts on a regular basis and immediately upon becoming aware of any unauthorized access to, or use of, its Services or Portal Account(s) or any other compromise involving Services or its Portal Account(s); and (ii) promptly apply any updates, upgrades, modifications or other Enhancements that Kaseya determines is necessary or appropriate to maintain the security, confidentiality, integrity, availability or performance of the Product.

7.66 If you provide us or Kaseya with reports, comments, suggestions, ideas or other feedback regarding the Services or our business, whether written or oral (collectively "Feedback"), you do so without any expectation of compensation. You hereby grant Kaseya a worldwide, irrevocable, transferable, perpetual, royalty-free right and license to use the Feedback to improve the Products, develop new Products and for any other purpose, including in all media now known and later developed. The provision of Feedback is strictly voluntary, and we are not required to hold it in confidence.

7.67 Notwithstanding any other provision in this Agreement or otherwise, and provided we comply with Applicable Law, Kaseya may evaluate and process use of Products and Content in an aggregated and anonymous manner, meaning in such a way that the individual is not or no longer identified or identifiable (referred to as "Aggregate Data"). Kaseya may use and share such Aggregate Data to improve the Products, develop new products, understand and/or analyse usage, demand, and general industry trends, develop and publish white papers, reports, and databases summarizing the foregoing, and generally for any purpose related to our business. Kaseya retain all Intellectual Property Rights in Aggregate Data. For clarity, Aggregate Data does not include personally identifiable

information or information that can identify any individual.

7.68 Administrative Data includes operational data and telemetry concerning use of the Products and Portals, such as information that servers record relating to the access and use of the Products and Portals. Administrative Data may include IP addresses, authentication tokens, machine identifications, access logs, device settings and Portal settings. Administrative Data is processed by Kaseya and the Supplier to provide and operate the Products and Portals, bill and invoice you, measure customer experience and adoption, monitor security, conduct investigations, develop new products and operate and improve our business, and you agree that we may use such Administrative Data for any such purpose.

Warranties and Representations

7.69 The Customer acknowledges and accepts that:

7.69.1 the only warranties provided to the Customer in respect of the Products are those which are stated within the **Kaseya Product Terms**; and

7.69.2 the remedies in respect of any breach of warranty are limited to those detailed within the **Kaseya Product Terms**.

7.70 The Supplier warrants that for a period of thirty (30) days from your first use of Software and Services, the Software and Services will operate substantially pursuant to the Documentation for the Software and Services. Warranty claims must be reported to the Supplier within the applicable Warranty period, and defects must be capable of being observed or reproduced by Kaseya. The Supplier and Kaseya's obligations and your sole remedy with respect to any valid Warranty claim is limited to one of the following as determined by Kaseya: (i) repairing the defect; (ii) replacing Product with product or services that are equivalent in performance and reliability; or (iii) in the case of Service Subscriptions, terminating the Subscription and issuing a credit for prepaid amounts or, in the case of hardware, issuing a credit for the hardware upon its return to Kaseya.

7.71 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SUPPLIER AND KASEYA DISCLAIM ALL OTHER PROMISES, REPRESENTATIONS AND WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SYSTEM INTEGRATION, DATA ACCURACY, DATA SECURITY, OR ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. WE DO NOT WARRANT THAT THE PRODUCTS WILL MEET ANY END USER, CUSTOMER OR OTHER REQUIREMENTS OR THAT THE OPERATION OF ANY PRODUCT WILL BE SECURE, UNINTERRUPTED, OR ERROR-FREE, FREE OF HARMFUL COMPONENTS OR THAT ALL ERRORS WILL BE CORRECTED. PRODUCTS ARE TOOLS FOR ASSISTING CUSTOMERS RUN AND PROTECT THEIR BUSINESSES OR THOSE OF THEIR CLIENTS, AND ARE NOT A SUBSTITUTION FOR APPROPRIATE INSURANCE, SUCH AS CYBER LIABILITY OR PROFESSIONAL LIABILITY INSURANCE. PRODUCTS ARE NOT DESIGNED OR INTENDED FOR USE IN LIFE DEPENDENT OR HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE SUCH AS THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS WHERE THE FAILURE OF THE PRODUCT COULD LEAD TO DEATH, PERSONAL INJURY, PHYSICAL DAMAGE OR ENVIRONMENTAL DAMAGE. EXCEPT FOR REPRESENTATIONS SPECIFICALLY MADE BY THE SUPPLIER OR KASEYA IN WRITING, WE MAKE NO REPRESENTATIONS OR WARRANTIES ABOUT ANY PRODUCT'S COMPLIANCE WITH LAWS AND REGULATIONS THAT ARE SPECIFICALLY APPLICABLE TO ANY END USER OR INDUSTRY AND DISCLAIM ALL LIABILITY ASSOCIATED THEREWITH. THE PRODUCTS MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. WE ARE NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NO SUPPLIERS OF ANY THIRD-PARTY COMPONENTS INCLUDED IN THE PRODUCTS WILL BE LIABLE FOR ANY DAMAGES WHATSOEVER.

Data Protection

7.72 Paragraphs 7.72 to 7.75 are supplemental to clause 10 of the **General Conditions** and which relates to processing of Personal Data by the Supplier as its Customer. This paragraph 7 specifically relates to Personal Data which is shared with the Supplier and Kaseya in the context of the provision or receipt of Services to the Customer.

7.73 The Supplier and Kaseya are each Processors in respect of the Customer Data. The Customer acknowledges and accepts the terms of Kaseya's Privacy and Security Terms and Data Protection Addendum.

7.74 The Customer acknowledges and agrees that Kaseya may host its product management portals and platforms in the United States regardless of where the Customer are its End Users resident or where the Services are used.

7.75 The Customer shall (i) notify the individual users of the Products that their Personal Data may be Processed for the purpose of disclosing it to law enforcement or other governmental authorities when required by Applicable Law as determined by Supplier; and (ii) obtain individual users' consent to the same.

Indemnities

7.76 The Supplier agree to defend the Customer from and against (or at our option settle) any third-party claims that a Service in the form supplied to you under this Agreement infringes or misappropriates a third party's patent, copyright or trademark rights and we will indemnify and hold you harmless from all damages, costs, and similar liabilities ordered by a court or agreed upon in settlement in connection with any such claim. Our indemnification obligations will not apply to (i) claims of infringement to the extent based on your combination of the Services with other products, services, software or marks if the infringement could have been avoided by the use of such Service not in such combination; (ii) any modifications to the Services not made by us; (iii) any damages incurred as a result of your failure to use any update to the Services we provide; (iv) use of a Services in a manner that does not conform to its Specifications; or (v) a Product-related claim stemming from your specific directions (these exceptions (i) through (v) collectively will be referred to as "IP Exclusions"). If we determine that a Service is or may be subject to an infringement claim, we may, at our option: (1) procure for you the right to continue using or distributing the Service in accordance with this Agreement or (2) replace or modify the Service so it becomes non-infringing. If we determine that neither of these options is commercially practicable, we may terminate this Agreement or your ability to further use or distribute such Product upon written notice to you. This paragraph represents your sole and exclusive remedy and the Supplier and Kaseya's sole and exclusive liability for any claims based on Kaseya's infringement of intellectual property or other proprietary rights.

7.77 The Customer agrees to defend the Supplier, Kaseya its licensors and Affiliates, and the officers, directors, employees and representatives of each of them (each a "Indemnified

Party"), from and against all damages and costs incurred as a result of a third-party claim and the Customer will indemnify and hold all Indemnified Parties harmless from all damages, costs, and similar liabilities in connection with any such claim, to the extent the claim arises out of (i) the Customer's breach of this Agreement; (ii) the Customer's negligence or other acts or omissions resulting, in whole or in part, in a third party claim being asserted against us; (iii) any of the IP Exclusions above; (iv) your actions in excess of the authority granted to the Customer by any End User; (v) the Customer's failure to secure Content, any personally identifiable information or Confidential Information in a reasonable manner (such as, for example, your failure to encrypt in transit or at rest when available or properly protect passwords or other access credentials); (vi) the Customer's breach of Applicable Law involving the Services; and (vii) except for claims of infringement or misappropriation for which we are under the terms of this Agreement, a claim brought by any of your End Users (both organizations or individuals) arising out of or related to the End User's relationship with you.

7.78 The foregoing indemnification obligations are conditioned on any of the indemnified parties: (i) notifying the indemnifying party promptly in writing of such action; (ii) reasonably cooperating and assisting in such defence; and (iii) giving sole control of the defence and any related settlement negotiations to the indemnifying party with the understanding that the indemnifying party may not settle any claim in a manner that admits guilt or otherwise prejudices the indemnified party, without consent.

PART E – TERMS APPLICABLE TO ALL SERVICES

8. UPGRADES AND ENHANCEMENTS

8.1 Subject to paragraph 8.4, where Upgrades are made to the Customer Network and/or Supported Equipment by the Supplier, they shall be deemed to be included in the definition of Supported Equipment and shall become subject to the terms of this Schedule for the remainder of the Term from the date of the Upgrade.

8.2 The Charges shall be increased to such sum as the Supplier shall require taking account of the Upgrade referred to in paragraph 8.1 above.

8.3 The Customer shall notify the Supplier in writing forthwith of any Upgrade made to the Customer Network and/or Supported Equipment or Software which is installed by any Third-Party Supplier.

8.4 Upgrades made to the Customer Network and/or Supported Equipment shall be included within the definition of Supported Equipment only after a report prepared by the Engineer of the Supplier on the effect of the Upgrade on the Customer Network and/or Supported Equipment has been produced and the Supplier has confirmed it is satisfied with the report.

8.5 The Supplier reserves the right, at its complete discretion, to exclude any such third-party Upgrades from becoming subject to the terms of this Schedule.

8.6 The inspection and report referred to in paragraph 8.4 shall be charged to the Customer at the rate specified by the Supplier from time to time and shall be paid in addition to the Charges referred to in paragraph 10 below.

9. CHANGE MANAGEMENT

9.1 The Supplier upon request by the Customer can undertake Change Requests and will manage all changes covered under the Services from scoping to release and testing in accordance with the Change Request process.

9.2 The Customer shall submit a Change Request through the Service Desk, subject to Additional Charges as follows:

9.2.1 Elective Changes on a fixed cost basis for common changes that do not require a detailed scope of works; and

9.2.2 Customised Changes are specific to the Customer and are scoped on a case-by-case basis with the Customer being charged on a time and materials basis.

9.3 All Elective Changes are completed on a time/materials basis and charged to the Customer as per the Supplier's Standard Schedule of Rates.

9.4 The Customer may also purchase, at the Commencement Date, a specific quantity of Technical Attendance Days which will be set out in the applicable Order.

9.5 For the avoidance of doubt, Customised Changes under paragraph 9.2.2 above shall be outside of the scope and terms of this Schedule and subject to a separate Order, will be specified and carried out in accordance with **Schedule 4.2 (Professional Services).**

10. CHARGES AND PAYMENT

10.1 This paragraph 10 is supplemental to clause 6 of the **General Conditions**. If this paragraph 10 expressly conflicts with clause 6 of the **General Conditions**, this paragraph 10 shall take precedence. The Supplier shall invoice the Customer for the Charges for the Services as set out in paragraph 10.2 in the amounts specified in the applicable Order or as varied under the terms of this Agreement.

10.2 Unless stated otherwise in the applicable Order, the Supplier shall invoice the Customer as follows:

10.2.1 Installation Charges, on or after the Commencement Date;

10.2.2 Recurring Charges annually in advance;

10.2.3 Usage Charges monthly in arrears;

10.2.4 Licence Fees annually in advance;

10.2.5 Additional Charges monthly in arrears;

10.2.6 any charges for Hardware, Devices and/or Software at the time of delivery of such Hardware, Devices and/or Software;

10.2.7 all reasonable and properly incurred expenses, including but not limited to travel and other out-of-pocket expenses;

10.2.8 reasonable time spent by the Engineer(s) in travelling, where the distance travelled is further than 35 miles from the Chess Office closest to the geographical location of the Customer Site; and

10.2.9 any Termination Charges upon termination of the Services.

hereinafter defined as **"Charges".**

10.3 The Customer acknowledges and agrees that Licence Agreements can take up to sixty (60) days to be processed with the Third-Party Supplier.

10.4 Additional Charges shall be invoiced in arrears at the end of the month in which the Additional Charges are incurred, together with replacement parts and any other expenses and costs reasonably incurred.

10.5 The Supplier shall have the right to invoice Additional Charges to the Customer for any expenses and costs reasonably incurred under paragraphs 5.34 and 11, or where the Supplier upon investigation an Incident is caused by something which the Supplier is not responsible for under this Schedule.

10.6 Unless otherwise stated in the Order, the Customer shall pay, by direct debit, each undisputed invoice (or such undisputed part thereof) within seven (7) days of the date of the invoice without any set-off or deduction.

10.7 Where the Customer in good faith disputes the Charges, the Customer shall notify the Supplier in writing within seven (7) days of the date of the invoice, in accordance with clause 6.17 of the **General Conditions**.

10.8 All Charges payable under this Schedule are exclusive of VAT which shall be paid by the Customer at the rate and in the manner prescribed by law.

10.9 If in the opinion of the Supplier, the Services are required by the Customer as a result of any misuse or neglect of, or accident to the Customer Network and/or Supported Equipment or due to the Customer not adhering to paragraph 3, or other third-party hardware problems, the Supplier reserves the right to charge Additional Charges in relation to the provision of the Services.

10.10 The Supplier reserves the right to charge the Customer an Additional Charge for an Incident where Supported Equipment has been moved to a new location and not installed by the Supplier, if the Supplier reasonably determined that the problem was caused by transportation or re-installation of the Supported Equipment.

11. EXCLUSIONS

11.1 Notwithstanding any other provision of this Schedule, the Supplier shall not be obliged to perform or provide the Services in one or more of the following circumstances:

11.1.1 the Customer is in breach of its obligations under paragraph 3 above or is in material breach of this Agreement;

11.1.2 negligence of the Customer or its End Users or the improper use by the Customer or its End Users of the Customer Network and/or Supported Equipment;

11.1.3 damage to the Supported Equipment resulting from accident, transportation or relocation, neglect, misuse or causes other than ordinary use (including but not limited to, failure to observe any instructions supplied by the manufacturer regarding the operation and maintenance) of the Supported Equipment;

11.1.4 damage caused by consumable items such as recording materials, machine stationary, ribbons, media, laser drum, toner, printer cartridges, paper trays, platen knobs, fuses, batteries, print heads, cathode ray tubes, switch boxes, power adaptor blocks or any other item considered to be a consumable by the Supplier;

11.1.5 damage caused by the use of non-manufacturer approved consumables, where this results in abnormal wear or damage to the Supported Equipment;

11.1.6 damage caused by virus attacks or failure due to any unauthorised third party Software;

11.1.7 alteration, modification, repair or maintenance of the Customer Network and/or Supported Equipment by any person other than the Supplier or its approved Third Party Supplier;

11.1.8 the Supported Equipment is removed from Site without the prior written approval of the Supplier;

11.1.9 insufficient or improper access to the Customer Network and/or Supported Equipment;

11.1.10 failure or fluctuations in electrical power supply and/or unsatisfactory environmental conditions which do not meet manufacturers' requirements;

11.1.11 where the Customer's own insurance covers the accidental or malicious damage to the Supported Equipment and costs relating to the Supported Equipment; and

11.1.12 damage to the Customer Network and/or Supported Equipment due to accidental damage, theft, vandalism or a Force Majeure Event.

11.2 Where the Supplier is called out in connection with any of the matters referred to in paragraph 11.1 or where the Supplier determines that the call was not warranted, the Supplier has the right to charge the Customer for time spent, any expenses and costs reasonably incurred as Additional Charges.

11.3 For the avoidance of doubt, the excluded events listed in paragraph 11.1 above shall not be counted or considered in relation to the performance of any Service Levels.

12. LIABILITY

12.1 THIS PARAGRAPH 12 IS SUPPLEMENTAL TO CLAUSE 9 OF THE **GENERAL CONDITIONS** AND IN THE EVENT THIS PARAGRAPH CONFLICTS WITH CLAUSE 9 OF THE **GENERAL CONDITIONS**, THIS PARAGRAPH 12 SHALL TAKE PRECEDENCE.

12.2 THE EXCLUSIONS AND LIMITATIONS OF LIABILITY SET FORTH IN THIS PARAGRAPH 12 FORM THE ESSENTIAL BASES OF THIS AGREEMENT AND HAVE BEEN RELIED UPON BY BOTH PARTIES, AND ABSENT SUCH EXCLUSIONS AND LIMITATIONS OF LIABILITY, THE TERMS OF THIS AGREEMENT AND THE CHARGES APPLICABLE TO THE SERVICES WOULD BE SUBSTANTIALLY DIFFERENT.

12.3 THE SUPPLIER DOES NOT GUARANTEE THAT THE SERVICES WILL PREVENT OR ISOLATE ALL CYBER THREATS AND IN NO CIRCUMSTANCES WILL THE SUPPLIER BE LIABLE FOR ANY LOSSES OR DAMAGES INCURRED BY THE CUSTOMER IN RELATION TO SUCCESSFUL CYBER THREAT AGAINST THE CUSTOMER'S SYSTEMS.

12.4 THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT ISOLATION OF THREATS MAY DISRUPT ITS BUSINESS OPERATIONS, INCLUDING ITS SYSTEMS, AND THAT THE IN NO CIRCUMSTANCES SHALL THE SUPPLIER BE LIABLE FOR ANY DOWNTIME OR BUSINESS DISRUPTION ARISING FROM STEPS TAKEN TO ISOLATE A CYBER THREAT.

12.5 THE SUPPLIER SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE SUSTAINED OR INCURRED BY THE CUSTOMER, ITS END USERS, OR ANY THIRD PARTY (INCLUDING WITHOUT LIMITATION ANY LOSS OR USE OF THE SUPPORTED EQUIPMENT OR LOSS OR CORRUPTION OF THE CUSTOMER'S PROGRAMS OR DATA) RESULTING FROM ANY BREAKDOWN OF OR FAULT IN THE SUPPORTED EQUIPMENT OR INHERENT OR PRE-EXISTING DEFECTS IN THE SUPPORTED EQUIPMENT, UNLESS SUCH A BREAKDOWN OR FAULT IS CAUSED BY THE NEGLIGENCE OR WILFUL MISCONDUCT OF THE SUPPLIER, ITS EMPLOYEES, AGENTS OR SUB-CONTRACTORS OR TO THE EXTENT THAT SUCH LOSS OR DAMAGE ARISES FROM ANY UNREASONABLE DELAY BY THE SUPPLIER IN PROVIDING THE SERVICES AND THEN ONLY TO THE EXTENT NOT OTHERWISE EXCLUDED BY THIS SCHEDULE.

12.6 THE CUSTOMER SHALL INDEMNIFY THE SUPPLIER AND KEEP THE SUPPLIER FULLY AND EFFECTIVELY INDEMNIFIED IN FULL ON DEMAND AGAINST ALL COSTS, CHARGES, DAMAGES AND OR ANY LOSSES SUSTAINED OR INCURRED BY IT ARISING DIRECTLY OR INDIRECTLY FROM THE CUSTOMER'S FAILURE TO PERFORM OR DELAY IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS SCHEDULE OR FROM ANY FRAUDULENT OR NEGLIGENT ACT OR OMISSION OR WILFUL MISCONDUCT OF THE CUSTOMER, ITS END USERS, EMPLOYEES, AGENTS OR SUBCONTRACTORS.

12.7 SUBJECT TO CLAUSE 9 OF THE **GENERAL CONDITIONS** (EXCEPT CLAUSE 9.4 WHICH IS SUPERSEDED BY THIS PARAGRAPH 12.7), THE MAXIMUM LIABILITY OF THE SUPPLIER, IN TORT, CONTRACT OR OTHERWISE ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS SCHEDULE SHALL BE LIMITED IN AGGREGATE TO A SUM EQUAL TO:

12.7.1 THE CHARGES PAYABLE UNDER THIS SCHEDULE DURING THE CALENDAR YEAR IN WHICH THE RELEVANT CLAIM ARISES; OR

12.7.2 FIVE HUNDRED THOUSAND POUNDS (£500,000) WHICHEVER IS THE HIGHER.

12.8 THE SUPPLIER SHALL NOT BE LIABLE TO THE CUSTOMER

FOR ANY LOSS ARISING OUT OF ANY FAILURE BY THE CUSTOMER TO KEEP FULL AND UP TO DATE SECURITY COPIES OF THE COMPUTER PROGRAMS AND DATA IT USES IN ACCORDANCE WITH GOOD INDUSTRY PRACTICE.

12.9 THE SUPPLIER SHALL NOT BE LIABLE FOR FAILING TO PERFORM THE SERVICES OR DELAYING THE SERVICES HEREUNDER BY REASONS OF FORCE MAJEURE. IF A FORCE MAJEURE EVENT PREVENTS THE SUPPLIER FROM PROVIDING THE SERVICES FOR MORE THAN THREE (3) MONTHS, THE SUPPLIER SHALL, WITHOUT LIMITING ITS OTHER RIGHTS AND REMEDIES, HAVE THE RIGHT TO TERMINATE THIS SCHEDULE IN RELATION TO ANY AFFECTED SERVICES IMMEDIATELY BY GIVING WRITTEN NOTICE TO THE CUSTOMER.

13. TERMINATION

13.1 This paragraph 13 is supplemental to clauses 2 and 8 of the **General Conditions.** If this paragraph 13 conflicts with clauses 2 and 8 of the **General Conditions**, this paragraph shall take precedence.

13.2 The Customer may terminate the Services generally or in relation to any part of the Services at any time by giving the Supplier not less than ninety (90) days' written notice prior to the end of the Minimum Term or Successive Term, such notice to take affect at the end of the Minimum Term or Successive Term.

13.3 The termination of one or more element of the Services shall not affect the continuing in effect of the remaining Services, including but not limited to the Supplier's obligation to perform the remaining Services and the Customer's obligation to perform its responsibilities and make payment of the Charges in accordance with this Schedule.

13.4 In the event of termination pursuant to paragraph 8.1.1 of the **General Conditions**, the Customer shall not be entitled to reimbursement of any aspect of the Charges as shall have been paid in advance and relate to the Services.

13.5 Where the Customer terminates the Agreement and/or the Services within its Minimum Term or Successive Term, the Supplier shall be entitled to invoice the Customer for Termination Charges in accordance with clause 8.7 of the **General Conditions**, or in alternative the Supplier shall be entitled to continue to invoice the Customer for the Charges in accordance with the Order for the remainder of the Minimum Term or Successive Term.

13.6 During the Minimum Term and Successive Term, the Customer is not permitted to reduce the number of Supported End Users or Equipment for the Services. Where the Customer cancels or terminates Services within the Minimum Term or Successive Term, Termination Charges shall be payable. The Customer may increase the quantity of Supported End Users or Equipment. Any increase is subject to the same terms as the existing Minimum Term or Successive Term and will expire on the same date as the existing Supported End Users and Equipment as applicable.

13.7 Where Services and/or the Agreement are terminated, the Supplier reserves the right to permanently delete all related Content or disable access to such Content from any remotely located servers owned by us or under our control, and we shall not be liable for such actions.

SAAS PROTECTION

13.8 Upon any termination of the Agreement or Services (as applicable), the Customer will immediately discontinue all use of the SaaS Protection Service.

13.9 For up to sixty (60) days after the effective date of termination, the Supplier will, upon written request allow the Customer to export or download a copy of its Backed-Up Data as provided in the Specifications. After such period, the Supplier has no obligation to maintain or provide any Backed-Up Data and may thereafter delete or destroy all copies of the Backed-Up Data, unless legally prohibited.

14. PEOPLE

14.1 The Customer shall not, without the prior written consent of the Supplier, at any time during the Term of this Schedule nor for a period of six (6) months following its expiry Or termination for any reason, solicit or entice away from the Supplier or employ any person who is, or has been, engaged as an employee of the Supplier at any time during such period. Any consent given by the Supplier shall be subject to the Customer paying the Supplier a sum equivalent to one hundred per cent (100%) of the then current annual remuneration of the Supplier's employee.

14.2 The Customer acknowledges and agrees that TUPE shall not apply to the Services and prior to the Commencement Date, all considerations, claims, actions or otherwise have been provided to the Supplier in relation to the effects, actions or claims of any TUPE and that the Customer indemnifies in full and holds the Supplier harmless of any such actions or claims of TUPE against the Supplier for business transfers or service provision changes for the Term of this Schedule and for a period of six (6) months following expiry or termination of this Schedule.

15. PROFESSONAL SERVICES

15.1 Where the Supplier has agreed to provide Professional Services, these services shall be subject to a separate Order and will be specified and carried out in accordance with **Schedule 4.2 (Professional Services)**.

ANNEX 1 - DEFINITIONS

Additional Charges means the additional charges incurred in accordance with terms of this Schedule together with any replacement parts and any other costs or expenses reasonably incurred if not expressly included in the relevant Order**;**

Administrator means one or more persons or entities authorised by the Customer to manage or use the SaaS Protection Service on behalf of the Customer, including access to and control of Backed Up Data. The Customer may have multiple Administrators, and we expressly rely on the authorisation and instruction of any Administrator until we receive written instructions to the contrary;

Administrative Data means data concerning registration, use and administration of Services that we or Kaseya may capture. For example, Administrative Data includes telemetry, logs that we keep regarding access to and use of the Portals and Products, as well as access to and downloading of Content. Administrative Data does not include the Content itself;

Advanced Software Management means the Advanced Software Management module which integrates an expanded library of software applications and enables both installation and uninstallation via a Software Management policy further described at Advanced Software Management;

API means an application programming interface;

Applicable Law means any legislation, authorisations, permissions, rules and regulations, codes of practice, orders and guidelines relating to the provision of the Infrastructure Support Services, including any directives or other requirements issued by any regulator from time to time;

Applications means a computer software package that performs a specific function directly for and End User or, in some cases, for another application, also referred to as an application program or application software;

Audit means the infrastructure audit as further detailed in paragraphs 2.4 to 2.8;

Backed-Up Site means a Third-Party Supplier application or service with which the SaaS Protection Service interacts, upon Customer's authorisation, to obtain copies of the Backed-Up Data;

Beyond Repair means where the Customer Network and/or Supported Equipment is at the end of its normal, useful working life, for which parts are no longer reasonably, commercially available or which is beyond economical repair;

BullPhish ID means a Phishing simulation and security awareness training platform that helps employees recognise and avoid email-based threats. Further described in Kaseya's published service terms available at: Terms of Use | ID Agent

Change Request means a formal request to change, modify or alter the Services provided by the Supplier to the Customer as set forth in the applicable Order;

Charges has the meaning given to it in paragraph 10.2;

Chess' PSA Platform means the Supplier's professional services automation platform used to deliver the Services;

Confidential Information means all operational written or oral information, disclosed by either party to the other that has been identified by the disclosing party as confidential or that by the nature of the circumstances surrounding disclosure ought reasonably to be treated as confidential, but not including Feedback, Aggregate Data, Log Data or Backed-Up Data;

Content means all data and other content that is submitted through the Services, platforms or otherwise made available to Kaseya through use of the Services by you, by an End-User, or on behalf of you or an End-user. An example of Content is your data that you may back-up through one of our backup Products;

Contract Year means a period of twelve (12) months from the Commencement Date and/or any subsequent anniversary of the Commencement Date;

Customer Data means all data, including text, sound, video, or image files, and software, that are provided to the Supplier and/or Kaseya by, or on behalf of, the Customer through use of the Services;

Customer Equipment means any equipment including purchased Hardware, Devices and Software used by the Customer in connection with the provision of the Services;

Customer Network means the Customer's physical network and server infrastructure, including (if any) servers and switches to routers and firewalls, plus business systems software;

Customised Changes has the meaning given to it in paragraph 9.2.2;

Dark Web ID means a monitoring tool that continuously searches the dark web for exposed credentials associated with your business domains. Further described in Kaseya's published service terms available at: Terms of Use | ID Agent

Datto EDR and Anti-Virus Services means Endpoint detection and Response combined with traditional antivirus capabilities to detect, respond to and remediate endpoint threats. Further described in Kaseya's published service terms available at: Datto EDR, Datto AV, Ransomware Detection Product Terms | Datto

Datto RMM means a Datto Remote Monitoring and Management (RMM) is a secure cloud-based RMM platform. Further described in Kaseya published service terms available at PSA, Datto RMM and Kaseya Quote Manager Terms of Use | Datto;

Datto Saas Protection means a cloud-to-cloud backup solution that protects Microsoft 365 and Google Workspace data from loss due to accidental deletion, ransomware, or malicious activity. Further described in Kaseya's published service terms available at: DATTO SAAS PROTECTION AND DATTO SAAS DEFENSE TERMS OF USE | Datto;

Device means any mobile handset, laptop, tablet, computer or other input item or handheld equipment, including all peripherals, excluding SIM cards and Applications, which are in the scope of the Services, as set out in the Order;

Elective Changes has the meaning given to it in paragraph 9.2.1;

Enhancement means any upgrade, update or modification to the SaaS Protection Service. All Enhancements will be subject to the terms in this Schedule;

Equipment means the Supported Equipment and any additions and changes as shall from time to time be agreed in writing between the parties;

End User means anyone permitted by the Customer to use or access the Customer Network and/or the Customer Equipment;

Engineer means the Supplier's Personnel who is responsible for carrying out technical engineering duties either remotely or at a Customer's Site;

Escalation Support shall have the meaning given to it in paragraph 4.20 and **Annex 3**;

Excluded Events shall have the meaning given to it in paragraph 11;

Force Majeure shall have the meaning given to it in Clause 9.6 of the **General Conditions**;

General Conditions means the Supplier's standard terms and conditions for the provision of the Services as set forth on the Supplier's website at www.chessict.co.uk/legal and which form part of this Agreement;

Good Industry Practice means in relation to any undertaking and any circumstances, the exercise of that degree of skill and care which could be reasonably expected of a highly skilled and experienced professional;

Hardware means any and all computer and computer related hardware, including but not limited to, computers, servers, network switches, UPS units, firewalls and connect peripherals;

Incident means any event which is not part of the standard operation of the Customer Network and/or Supported Equipment and which

causes or may cause an unplanned interruption to, or a reduction in the quality of the performance of the Customer Network and/or Supported Equipment;

Incident Based Charges means the Charges payable pursuant to the Supplier's Standard Schedule of Rates where the Customer raises an Incident under Standard Support Incident Billing Model;

Incident Management is the process as further defined in paragraphs 4.9 to 4.12 that the Supplier follows to manage an Incident as set out in Annex 2;

Incident Support SOC Document means the document issued the Customer during the onboarding process and which the Supplier may update from time to time which details the Incident process applicable to the MDR Service;

Inky Email Security means an automated platform that protects from malicious data and phishing attacks powered by AI. Furthe described in Kaseya's published service terms available at INKY Product Terms of Use - Kaseya;

ITIL Methodology means a set of IT Service Management practices that focuses on aligning IT services with the needs of business;

Installation Charges means the charges in relation to the installation of the Services or any Customer Equipment as appliable;

Kaseya means Kaseya Limited, its subsidiaries, parent companies, and other affiliated entities from time to time;

Kaseya Product Terms means the additional terms that apply to the Customer's use of Kaseya Products available at Kaseya Legal Information - Terms, Policies and Solution Catalogs | Kaseya, and Kaseya Data Processing Addendum - Kaseya as updated from time to time;

Licence Agreement(s) means any licence or terms under which the Customer is permitted to use third party Software;

Licensed Device means the single physical hardware system to which a license is assigned. For the purposes of this definition, a hardware partition or blade shall be considered a separate licence;

Licence Fees means the charges associated with the use of the Software, by the purchase of a Licence Agreement;

Managed Detection and Response (MDR) Services means a managed security service providing 24/7 threat detection, analysis and response support via the RocketCyber Security Operations Centre (SOC). Further described in Kaseya's published service terms available at: RocketCyber Terms of Use - RocketCyber

Managed Services means the Services to be provided by the Supplier as further defined in **Part C** of this Schedule;

Managed Support Services means the services to be provided by the Supplier as further defined in **Part B** of this Schedule;

Operating System means system software that manages computer hardware, software resources, and provides common services for computer programs;

Order means an order, contract, or agreement issued by the Supplier to the Customer for the provision of the Services;

Portal means any web-based application, platform or portal provided by Kaseya or the Supplier that contains information related to Kaseya as well as the purchase, use, management, support and/or resale of the Services;

Product means all products identified in the **Kaseya Product Terms**, such as all Software, Kaseya Services and other web-based services;

Professional Services means engineering support as further detailed in **Schedule 4.2 (Professional Services)**;

Ransomware Detection means a tool that scans systems for signs of ransomware behaviour and alerts administrators before major encryption or damage occurs. Further described in Kaseya's published service terms available at: Datto EDR, Datto AV, Ransomware Detection Product Terms | Datto

RMM Agent means a lightweight software program installed on a device that supports agent installation, which gathers up-to-date information about the device's health and status;

RMM Platform means the Supplier's preferred real time, cloud-based system wide monitoring and management tool;

Recurring Charges means the Charges for the Services, or applicable part of the Services, including but not limited to the Standard Support Services, Managed Support Services, Managed Services and/or MSaaS, which are invoiced repeatedly in every billing period as set out in the Order;

Resolved or Resolution means where an Incident has been resolved and the standard operation of the Customer Network and/or Supported Equipment as is expected in accordance with manufacturers' recommendations;

SaaS Alerts means a cyber security monitoring platform for SaaS applications, alerting administrators to suspicious user activity across clous environments. Further described in Kaseya's published service terms available at: Product Terms of Use - SaaS Alerts;

Services means the Standard Support Services, Managed Support Services, Additional Services, Managed Services and MSaaS, where applicable;

Service Desk means the Supplier's service desk that the Customer is able to contact to report an Incident;

Service Levels means the relevant Service Level targets as further defined in **Annex 2** of this Schedule;

Site(s) means the Customer's premises at which the Customer Network and/or Supported Equipment is located as specified in the relevant Order;

Software means the software licensed to the Customer as specified in the Order, together with any embedded software which is necessary for provision of the Services and/or operation of the Supported Equipment, which may be provided by a Third-Party Supplier and governed by a separate Licence Agreement;

Standard Support Hours means 08:00hrs to 18:00hrs on a Working Day;

Standard Support Services means the standard support service as further defined in **Part A** of this Schedule;

Subscription means an enrolment for Kaseya Services for a defined Term as provided under this Agreement;

Supplier's Personnel means all employees, agents, consultants, sub-contractors and other representatives of the Supplier who are involved, or proposed to be involved, in the provision of the Services;

Support Hours means the various options for support hours available to the Customer as further detailed in paragraph 4.8 in **Part A** of this Schedule and as set out in the applicable Order;

Supported Equipment means the list of Customer Equipment, Hardware and/or Software as further detailed in the relevant Order in respect of which the Supplier shall provide the Services in accordance with this Schedule;

Technical Attendance Days means where an Engineer attends Site to carry out Elective Changes during Standard Support Hours, excluding consumables and spare parts;

Term means the Minimum Term as set forth in the applicable Order, together with any Successive Term;

Termination Charges mean any compensatory charges payable by the Customer to the Supplier upon termination of this Agreement, in whole or part, in accordance with clause 8.7 of the **General Conditions** and as set out in the applicable Order, or if not specified then an amount equal to 100% of the Recurring Charges for all remaining months for the Minimum Term, together with any waivered one-off charges or Installation Charges;

Third Party Supplier means a third-party supplier, provider or supplier of services of which:

(a) the Customer may utilise for the provision of Equipment and the Customer's Network, and;

(b) the Supplier may utilise for provision of the Services;

TUPE means the Transfer of Undertakings (Protection of Employment) Regulations 2006;

Upgrades means an enhancement to features or capabilities or performance of the Customer Network and/or Supported Equipment, such as the addition of memory, co-processors, optional cards, manufacturers modifications or any other changes to the technical specifications or configuration of the Customer Network and/or Supported Equipment;

Usage Charges means the Charges for the Services which are calculated by reference to the Customer's use of the services such as Incident Based Charges where the Customer has contracted for the Standard Support Incident Based Billing Model;

Use Rights means the use rights or terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. The Use Rights for Software are published by Kaseya in the Kaseya Product Terms.

ANNEX 2 – INCIDENT MANAGEMENT PROCESS

1. INCIDENT IDENTIFICATION

1.1 The Customer shall report an Incident to the Service Desk as soon as reasonably practicable by telephone, email or Chess' PSA Platform and tickets generated automatically, via the web/email function or manually inputted by the Supplier will be processed by the Service Desk.

1.2 The Supplier shall identify and classify if a request submitted to the Service Desk is either (i) an Incident or (ii) a Change Request as defined in Annex 1. All Incidents shall be managed in accordance with this Annex 2.

1.3 Where a request is deemed by the Supplier to be a Change request, the provisions of paragraph 9 of this Schedule 4.4 shall apply and unless otherwise stated in the Order, all Change Requests shall be chargeable to the Customer.

2. PRIORITY CLASSIFICATION

2.1 The Supplier shall allocate a unique reference number to each Incident and shall prioritise the Incident as follows:

PRIORITY LEVEL	DESCRIPTION
Priority 1 Critical	A critical service is non-operational, impacting the Customer's business, multiple End Users or multiple Sites; or severe functional error or degradation of Service(s) affecting production, demanding immediate attention. **Business Risk is High**
Priority 2 Major	The Customer's business is experiencing failure or performance degradation that impairs the operation of a critical business Service, although a work around may exist; or Application functionality is lost; or significant number of End Users or major Site is affected. **Business Risk is Medium**
Priority 3 Minor	The Customer is experiencing a problem that causes moderate business impact. The impact is limited to an End User or a small Site; or incident has moderate, not widespread impact; or involves partial loss with minimal impact which is non-critical in nature. **Business Risk is Low**
Priority 6 Change Request	Standard service request (e.g. End User guidance and Change Requests); or updating documentation. **Business Risk is Minor localised**

2.2 Subject to paragraph 1.3 above, the Supplier shall use reasonable endeavours to deliver a Change Request as soon as reasonably practicable during Standard Support Hours.

3. INVESTIGATION AND DIAGNOSIS

3.1 Tickets are generated automatically, via the web/email function or manually inputted and processed by the Service Desk through Chess' PSA Platform. Initial triage of the ticket, fact verification including incident prioritisation and classification are completed.

3.2 The Service Desk will then attempt to resolve or direct the Incident to the appropriate service team, which may include Escalation Support.

3.3 Escalation Support will include the transfer of a ticket to the appropriate service team, be that 2nd/3rd line field-based Engineers for on Site attendance, billing or provisioning or another internal team and/or Third-Party Suppliers. For Change Requests this may also include account management.

3.4 Throughout the Incident or Change Request, updates, notes and where appropriate log files and images will be placed on Chess' PSA Platform. The status of an Incident or Change Request will change depending on the current actions required.

3.5 If an Incident or Change Request requires input from the Customer, the ticket will be placed in a deferred state until a response is received.

4. RESOLUTION AND CLOSURE

4.1 When the Incident has been Resolved, the notes, including a description of the resolution will be updated and made available for review by the Customer if required.

4.2 Where appropriate communication will be made between all parties before the Incident is closed in accordance with Incident Management deliverables.

4.3 Incidents may also be closed, if after reasonable effort has been made to get a response from the Customer, no update has been given on three (3) consecutive occasions. In such cases Incidents can be reopened upon request by the Customer.

5. SERVICE LEVELS

5.1 The Supplier shall use its reasonable endeavours to ensure that response times to the Customer's notification of an Incident are not more than:

PRIORITY LEVEL	CATEGORY	RESPONSE TARGET[1] (NORMAL WORKING HOURS)
Priority 1	Critical	1 Hour
Priority 2	Major	4 Hours
Priority 3	Minor	8 Hours
Priority 6	Minor	5 Working Days

1. calculated from receipt of notification of Incident by Supplier

5.2 The response targets in paragraph 5.1 above are standard response targets. Where the Supplier has agreed specific response targets with a Customer, these shall be set out in the relevant Order.

ANNEX 3 - ESCALATION SUPPORT

1. 1st LINE ESCALATION SUPPORT

1.1 The Supplier shall provide to the Customer 1st line support, including the collation, checks and triage of Incidents by the Service Desk, with actions taken deemed to be moderate impact, low risk activities and dealt with as follows:

1.1.1 collecting the inbound request from the Customer via either Chess' PSA Platform or an inbound call to the Service Desk;

1.1.2 confirming the name, location, contact details of the End User reporting, are complete (including Data Protection checks competed for phone-based incidents);

1.1.3 confirming the specific details of the request are complete, and;

1.1.4 assigning a priority status in accordance with paragraph 2 of Annex 2

following the above, the Service Desk shall confirm if an action plan can be written for the request and if it can, then the ticket will be actions identified.

1.2 If the action plan fails to resolve the Incident, requires an Engineer on Site, a plan cannot be written or committed to (due to knowledge or access), the ticket will be escalated to the Supplier's customer service team (or nominated contact) to proceed with the initial request and resolve.

2. 3rd LINE ESCALATION SUPPORT

2.1 Where escalated tickets that have been logged and triaged by the Customer, then escalated to the Supplier via the Service Desk, due to unsuccessful resolution via the Customer's internal service team, the following must have been completed by the Customer prior to escalation:

2.1.1 all steps in paragraph 1 above have been documented in respect of 1st line escalation support;

2.1.2 document and supply all actions taken by the Customer's 2nd line or escalated service team;

2.1.3 document and supply all logs, screen shots, supporting information, and;

2.1.4 ensure that the documented priority for the Incident as stated in 1st line escalation is still current and correct

upon acceptance of the request by the Supplier, the Service Desk will review and manage the Incident.

2.2 The Supplier shall communicate with the Customer's service team or nominated contact to the point of Resolution of the Incident.

2.3 Where required the Service Desk will call upon the Customer's service team or nominated contact to complete local actions, where appropriate.