KRAYMA TECHNICAL SOLUTIONS LIMITED

CONDITIONS FOR THE SUPPLY OF SUPPORT SERVICES

SUPPORT SERVICES CONDITIONS

These Conditions apply to the supply, licence and support of software and hardware products, the supply of related equipment and the provision of system, development, managed and other ICT services by Krayma Technical Solutions Limited (company number 7674074) whose registered office is at 13 Spinners Court, West End, Witney, OX28 1NH ("**Krayma**") to the Client. These Conditions and the remainder of the Agreement apply to the exclusion of any other terms and conditions including any which the Client may attempt to introduce by way of purchase order or otherwise.

1. **Definitions**

1.1 In these Support Services Conditions, the following expressions will have the following meanings, unless inconsistent with the context:

"**Core Conditions**"	the "*Core Conditions of Supply*" of Krayma to which these Support Services Conditions are attached or appended.
"**Customer Service Centre Hours**"	as defined in the SLA
"**Support Services Conditions**"	these conditions (clauses 1 to 6) which are to be read in conjunction with the Proposal, Core Conditions, SLA and remainder of the Agreement.
"**Additional Support Services**"	any services provided by Krayma to the Client pursuant to clause 5 (if any)
"**Support Services Fees**"	the fees for the Support Services as set out in the Proposal, as amended from time to time in accordance with clause 5
"**Support Services**"	those helpdesk and reactive support services to be provided to the Client by Krayma pursuant to the Agreement, as described in these Support Services Conditions, the SLA, and the Proposal
"**Managed Software**"	that computer software specified in the Proposal in respect of which the Support Services are to be provided.
"Operational Guide"	that guide produced by Krayma for its customers further defining their use of the Support Services, as the same may be amended by Krayma from time to time.
"**SLA**"	the service level agreement for the Support Services, appended to the Agreement and which forms part of the Agreement.
"**Support Hours**"	as defined in the SLA

1.2 Terms and expressions not defined in these Support Services Conditions will unless the context otherwise requires have the meaning given to that term or expression in the Core Conditions or other set of Additional Conditions.

1.3 References in these Support Services Conditions to clauses will, unless stated otherwise, be to clauses of these Support Services Conditions.

2. Provision of Support Services

2.1 Krayma will provide the Support Services to the Client upon the terms and conditions of these Support Services Conditions, the SLA, and the remainder of the Agreement.

2.2 Without prejudice to the provisions of clause 10 of the Core Conditions, Krayma will provide the Support Services for the initial support period referred to in the Proposal (the "**Initial Support Period**") and will continue beyond that period, subject to termination by either party serving three months' written notice on the other to expire on the last day of the Initial Support Period or thereafter. The "Initial Support Period" is 12 months. Termination of the support agreement during the "Initial Support Period", other than to give notice at the end of the "Initial Support Period", will be at the sole discretion of Krayma Technical Solutions Ltd, unless there is a case of negligence on the part of Krayma Technical Solutions Ltd. After the "Initial Support Period", a party may terminate this contact by serving 2 months written notice.

2.3 Krayma will only be obliged to provide the Support Services:

2.3.1 during Support Hours.

2.3.2 if an Out of Hours Provision agreement is in place.

2.3.3 in relation to the Services Provided in the SLA.

2.4 Krayma will not be required to follow any system maintenance windows or routines designated by the Client for the provision of Support Services, unless agreed by Krayma in writing.

3. Limitations of the Support Services

3.1 The obligation of Krayma to provide the Support Services will not extend to:

3.1.1 any software or hardware or other equipment which does not form part of the Managed Support Service;

3.1.2 installation of new/additional software and hardware and other equipment, that is required by the client after the initial snapshot of the clients' infrastructure/configurations were taken at the outset of the support agreement.

3.1.3 Reconstitution or rectification of lost or corrupted data where the loss or corruption has resulted other than from the fault of Krayma.

3.1.4 Failure of the Client to implement reasonable recommendations in respect of or solutions to faults previously advised by Krayma.

3.2 Krayma will not be liable for any failure to provide the Support Services which arises as a result of the failure by the Client to comply with its obligations as set out in the Agreement.

3.3 Krayma will not be obliged to provide any services which are not Support Services, unless otherwise agreed with the Client in writing pursuant to clause 5.5.

4. Client's Obligations

4.1 During the continuance of the Agreement the Client will:

4.1.1 comply with the provisions of the SLA with regard to the provision of the Support Services.

4.1.2 fully back-up and validate all programs, data and records held or stored and retain security and back-up copies, in accordance with best computing practice. If Krayma provide a back-up solution for the client, then the client will be responsible for directing Krayma as to which data, records and information should be backed up under the agreement, and will confirm the correct data, information and records are backed up with regular backup platform reviews, as agreed between Krayma and the client. Recommended on a quarterly basis but no more frequently than monthly.

4.2 The Client shall if requested by Krayma provide staff familiar with the Client's programs and operations, who shall co-operate fully with Krayma' personnel in the diagnosis of any malfunction. The Client will provide to Krayma such information as it may require in relation to those parts not supplied by Krayma including accurate details of warranty cover for those parts.

5. **Support Services Fees**

5.1 Krayma will invoice the Client:

5.1.1 Monthly or annually in advance for the Managed Support Services Fees referred to in the Proposal; and

5.1.2 at the end of each calendar month for Additional Services provided in that month and Services which are referred to in the Proposal as being charged on a time and materials basis.

5.2 Krayma will not be obliged on termination of the provision of the Support Services to make any refund to the Client of any Support Services Fees paid in advance unless termination in accordance with Clause 10 of the Core Conditions is through the actions of Krayma. In this event Krayma will agree a refund with the Client that reflects the value of the Support Services paid for but not delivered. If the reason for termination cannot be agreed, both parties agree to resolve the issue in accordance with clause 12 of the Core Conditions.

5.3 If the Client does not pay the Support Services Fees in accordance with the provisions of the Agreement, Krayma may (without prejudice to its other rights and remedies available in connection with the Agreement) withhold provision of the Support Services until payment is made in full and cleared funds.

5.4 If there is a change to any of the matters set out in the Proposal affecting the provision of the Support Services including any of the assumptions of Krayma as to the provision of those Services, Krayma may revise the Support Services Fees to take account of such change.

5.5 Where:

5.5.1 Krayma agrees in writing to provide system support services to the Client in addition to the Support Services,

5.5.2 provides services in respect of any of the matters referred to in clause 3.1 or outside Support Hours,

the Client changes its requirements for the Support Services and Krayma agrees to accept that change, or where Krayma incurs additional obligations or time as a consequence of the Client's failure to comply with its obligations under this Agreement, then the Client will pay for those additional services at the standard rates of Krayma from time to time in force applicable to the provision of the services in question. No work will commence without prior agreement from the Client.

5.6 Where the SLA provides, the Client may redeem "service tokens" it purchases from Krayma by ordering from Krayma an agreed element of Support Services or other system support services which Krayma will provide for up to the relevant limit of Support Hours detailed in the SLA. Each token can only be redeemed once and must be redeemed within the relevant time period stated in the SLA.

6. **Warranty**

6.1 Krayma warrants that it will provide the Support Services and any additional Support Services as covered by both the Support Agreement and associated SLA, with reasonable care and skill (the "**Support Services Warranty**") and in accordance with Schedule 1 (ISO).

6.2 Krayma will only be liable for a breach of the Support Services Warranty where no Outstanding Monies remain payable (save where the Client has in writing raised a bona fide dispute) and the Client notifies Krayma in writing of a failure within 30 days of the Client becoming aware of the failure.

6.3 If the Client makes a valid claim against Krayma based on the failure of Krayma to comply with the Support Services Warranty, then Krayma will at its option take such steps as are necessary to remedy such failure. or refund such part of the Support Services Fees as relates to such services and will have no further liability for a breach of the Support Services Warranty.

6.4 Notwithstanding the provisions of clause 10 of the Core Conditions the aggregate liability of Krayma under or in connection with the Support Services Warranty and these Support Services Conditions will in no event exceed one times the Support Services Fees paid to Krayma during the preceding twelve-month period

SCHEDULE 1

ISO

1. Definitions.

Good Industry Practice	the exercise of that degree of skill, care, prudence, efficiency, foresight, and timeliness as would be expected from a leading company within the technology sector.
Client Data	All Client data and information to which Krayma is exposed pursuant to this Agreement.
Krayma Personnel	employees and contractors engaged by Krayma in the supply of its services to Client.

2. Krayma shall implement information security practice and a set of controls including access control, performance review, monitoring, reporting, and auditing, which comply with Good Industry Practice, as further specified by Client from time to time.

3. Krayma shall only be entitled to use Client Data in accordance with the terms of this Agreement and shall make no other use of Client Data.

4. Client Data shall be made available to Krayma Personnel on a need-to-know basis.

5. Krayma shall manage user access in accordance with Logical Access below.

6. Krayma shall implement information security practices which comply with the principles of ISO27001.

7. Krayma shall establish and implement an incident and problem management process in accordance with ICT incident and problem management below.

8. Krayma shall ensure that Krayma employees are trained in good information security practice on joining Krayma and at least annually thereafter.

9. Krayma shall ensure that, where it subcontracts services which are part of this Agreement, it shall a) have Client's prior written consent to do so, and b) shall impose on its subcontractors' obligations which are at least as onerous as those set out in this Schedule and this Agreement.

10. Krayma's contact person for information security issues is:

Name:	Nik Jarvis
Mobile:	01993 224400
Email:	njarvis@krayma.com

11. Krayma shall ensure that Krayma Personnel are vetted for identity and background on joining Krayma and at least annually thereafter.

12. Client shall be entitled to audit Krayma (and relevant subcontractors) so as to verify compliance with the terms of this Agreement.

13. Krayma shall, at least once every 2 years, at their own cost use an independent third party to audit the effectiveness of its information security controls.

14. Where either Client's audit or the third-party audit reveals any material defects, Krayma shall promptly and at its own cost remedy such material defects.

(1) LOGICAL SECURITY

Krayma shall define, document, and implement procedures for logical access control (identity and access management). These procedures shall be implemented, enforced, monitored, and periodically reviewed. The procedures shall also include controls for monitoring anomalies. These procedures shall, at a minimum, implement the following elements, where the term 'user' also includes technical users:

a) **Need to know, least privilege and segregation of duties:** Krayma shall manage access rights to information assets and its supporting systems on a 'need-to-know' basis, including for remote access. Users shall be granted minimum access rights that are strictly required to execute its duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

b) **User accountability:** Krayma shall limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems. This goes against Microsoft best practice, which limits Global Admin to 5 max.

c) **Privileged access rights:** Krayma shall implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems shall be granted only on a need-to-know basis and when strong authentication solutions are used.

d) **Logging of user activities:** at a minimum, all activities by privileged users shall be logged and monitored. Access logs shall be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets. Krayma shall use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.

e) **Access management:** access rights shall be granted, withdrawn, or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed. In the case of termination of employment, access rights shall be promptly withdrawn.

f) **Access recertification:** access rights shall be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.

g) **Authentication methods:** Krayma shall enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods shall be commensurate with the criticality of ICT systems, information or the process being accessed. This shall, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

(2) ICT INCIDENT AND PROBLEM MANAGEMENT

Krayma shall establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable Krayma to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Krayma shall determine appropriate criteria and thresholds for classifying events as operational or security incidents, as well as early warning indicators that shall serve as alerts to enable early detection of these incidents.

To minimise the impact of adverse events and enable timely recovery, Krayma shall establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling, and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process shall establish:

a) the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;

b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);

c) problem management procedures to identify, analyse and solve the root cause behind one or more incidents — Krayma shall analyse operational or security incidents likely to affect Krayma that have been identified or have occurred within and/or outside the organisation and shall consider key lessons learned from these analyses and update the security measures accordingly;

d) effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints — to ensure that:

   i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to Client promptly;

   ii) Client is promptly informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response, and the additional controls to be defined as a result of the incidents.

e) incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;

f) specific external communication plans for critical business functions and processes in order to:

   i) collaborate with relevant stakeholders to effectively respond to and recover from the incident;

   ii) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.