TRITAN SOFTWARE INTERNATIONAL
ENTERPRISE SOFTWARE LICENSE & SERVICES AGREEMENT

TRITAN provides software solutions for the maritime industry ("**Solutions**"). The Solutions include software and services designed to assist clients with the operation of a fleet of maritime vessels. Client operates a fleet of maritime vessels and such operations require the Client to support and provide certain services to onboard and shoreside personnel as well as to monitor, record and process certain operational, compliance and management information related to operation of the maritime vessels and to the provision of the related services ("**Client Operations**"). Client Operations are conducted both onboard the Client's vessels by onboard personnel and shoreside by personnel at various shoreside facilities. Throughout the Term, as defined in Section 5.0 of the General Terms, of this Enterprise Agreement, TRITAN and Client may be referred to herein collectively as the "**Parties**" or individually as a "**Party**."

This Enterprise Agreement sets forth the terms and conditions under which TRITAN will make the Solutions available to Client, and will serve as the controlling document under which Client and Client's Affiliates may license software and procure services from TRITAN by entering into one or more appropriate order, statement of work, work order, purchase order, or other mutually agreeable document entered into by the parties and expressly incorporating this Enterprise Agreement (each an "**Order**"). To the extent conflicts or inconsistencies exist between this Enterprise Agreement and an Order, the provisions of this Enterprise Agreement shall govern and control.

To the extent Client is subject to the US Health Insurance Portability & Accountability Act ("HIPAA"), the Parties will enter into, and this Enterprise Agreement will be subject to the terms of the ***<<HIPAA Business Associate Agreement>>*** appearing below. To the extent the Client is subject to EU General Data Protection Regulation ("**GDPR**"), the Parties will enter into, and this Enterprise Agreement will be subject to the terms of the ***<<GDPR Processing Terms>>*** appearing below.

License Grant. Subject to the ***<<License Terms>>*** and the ***<<Terms and Conditions>>***, both appearing below, TRITAN grants Client a worldwide, non-exclusive, non-sublicensable, non-transferable license to allow Client's Authorized Users to use the Software incorporated in the Solutions identified in the applicable Order solely for Client's internal business purposes.

Support and Maintenance. Subject to the ***<<Support Terms>>*** and the ***<<Terms and Conditions>>***, both appearing below, TRITAN will provide the Support and Maintenance Services ("**Support Services**") for the Solutions as identified in the applicable Order.

Hosting and Data Management. Subject to the ***<<Hosting Terms>>*** and the ***<<Terms and Conditions>>***, both appearing below, TRITAN will provide the Hosting and Data Management Services ("**Data Services**") for the Solutions as identified in the applicable Order.

Data Processing. Certain Data Processing Services are required as part of the Solutions, including, but not limited to, the processing of the Personal Data ("**Data Processing Services**"). Subject to the ***<<Data Processing Terms>>*** and the ***<<Terms and Conditions>>***, both appearing below, TRITAN will provide the Data Processing Services required for the Solutions identified in the Order.

Consideration. Client shall pay TRITAN all fees ("**Fees**") set forth in this Enterprise Agreement and applicable Orders without offset or deduction, including, but not limited to the Software License Fees, the Support and Maintenance Fees, the Hosting and Data Management Fees, the Professional Services Fees, the Supplemental Services Fees and any applicable expense reimbursements as provided for in the ***<<Payment Terms>>*** appearing below.

Definitions. All capitalized terms used but not otherwise defined in this Enterprise Agreement shall have the meaning set forth in the ***<<Definitions>>***, appearing below, or in the Order (the "**Definitions**").

<<GENERAL TERMS>>

1.0 RELATIONSHIP STRUCTURE AND MANAGEMENT

1.1 Project Executive. Each Party shall designate a senior level individual who will be authorized to act as the primary contact for that Party and who will have authority to make decisions for the Party for any actions taken or decisions made in the ordinary course of operations (each a "**Project Executive**"). The Project Executive for each Party will be designated in the Enterprise Agreement. Each Project Executive may designate in writing other individuals to serve as points of contact for each Order, and the Project Executives will be identified in writing on each Order.

1.2 Governance Committee. Promptly following execution of each Order and when applicable, the Parties will appoint a committee (the "**Governance Committee**"), made up of a number representatives from each Party (inclusive of, but not limited to, each Party's Project Executive). The Governance Committee will be responsible for monitoring the progress of efforts under the applicable Order, for monitoring the success of the relationship between the Parties, and for undertaking of joint objectives pursuant to this Enterprise Agreement. The Governance Committee will also be responsible for initial efforts to resolve any disputes or disagreements arising under or related to this Enterprise Agreement.

1.3 Client Cooperation. Client understands and agrees that its cooperation is required for the timely delivery of the Solutions. Client will, to the extent required: (a) provide TRITAN with any necessary resources required to fulfill an Order, (b) provide TRITAN with any necessary and reasonable access to Client's personnel, materials, systems, facilities or data, (c) cause the appropriate personnel to reasonably cooperate with TRITAN as required for TRITAN to provide the Solutions, (d) abide by the terms and conditions of this Enterprise Agreement, and (e) make all undisputed payments when due.

1.4 Use by Affiliates. Client's Affiliates may license Software or procure Services from TRITAN by executing an Order in the same manner as the Client. When one of Client's Affiliates is licensing Software or procuring Services pursuant to an Order, all references in this Enterprise Agreement, including references in the relevant Order, to "**Client**" shall also refer to such Affiliate.

1.5 Use by Authorized Users. Client is responsible for ensuring each Authorized User's and each Client Location's compliance with the terms and conditions of this Enterprise Agreement and all applicable national, state, and local laws, rules and regulations, including, but not limited to, compliance with, where applicable, HIPAA, the HITECH Act and GDPR.

2.0 NO DELEGATION OF RESPONSIBILITIES.

2.1 Client acknowledges and agrees that the Solutions are not intended to, and shall not be deemed in any way to, eliminate, replace or substitute for, in whole or in part, the judgment of Client and/or Authorized Users, and Client shall have full responsibility for its business activities, and the actions or inactions of its employees, contractors, affiliates and clientele when performing those business activities, including, but not limited to, providing incident management, medical care, or financial assessments (together the "**Business Actions**"). Any reliance by Client's employees, contractors, affiliates and clientele on the Solutions in conjunction with their Business Actions shall not diminish Client's responsibility for its Business Actions.

2.2 The Solutions are not designed, intended, or authorized for use in any lifesaving or life sustaining systems, or for any other application in which the failure of the Solutions could create a situation where personal injury or death may occur. Should Client or any of its Authorized Users use the Solutions for any such unintended or unauthorized use, Client shall indemnify and hold TRITAN and its shareholders, officers, subsidiaries and affiliates harmless from and against all claims, costs, damages, and expenses, and reasonable attorneys' fees arising out of, directly or indirectly, any claim of product liability, personal injury or death associated with such unintended or unauthorized use of the Solutions, even if such claim alleges that TRITAN was negligent regarding the design or manufacture of the Software.

2.3 Acceptable Use Policy**.** Client shall have the sole responsibility to set usage/privacy guidelines for persons that may use or access the Software and/or Services on behalf of Client. TRITAN will notify Client, when required, of complaints received by TRITAN regarding an alleged violation of a usage or privacy policies. In such event, Client agrees that it will reasonably investigate all such complaints and take action necessary to remedy any violation consistent with the manner prescribed within usage or privacy policies and applicable law. TRITAN may communicate with Client's Project Executive regarding any such alleged violations. Client and each Affiliate shall post or make known its usage and privacy policies to employees, agents, representatives and contractors. Notwithstanding the foregoing, TRITAN shall be allowed to take appropriate action (e.g. suspension of Service or access to Software, only to the extent necessary to deal with a usage or privacy violation) upon as much advance notice as is practicable under the circumstances in the event TRITAN experiences a usage or privacy violation or if there is a threat which will materially and adversely affect the TRITAN Network.

3.0 NON-CLIENT DATA

Client agrees that as a result of Client's, its Affiliates' and their Authorized Users' use of the Solutions, TRITAN will collect data and information related to the Authorized Users' use or TRITAN's provision of the Solutions (the "**TRITAN Data**"). TRITAN shall be the

exclusive owner of all TRITAN Data. Client acknowledges and agrees that, subject to all applicable privacy laws, TRITAN Data may be used by TRITAN in an aggregated and anonymized manner for any purpose, including, but not limited to, compiling statistical and performance information related to the provision and operation of the Solutions.

4.0 ORDERS/CHANGE MANAGEMENT

4.1 New Work.

(a) Requests. Client shall submit all requests for new Solutions, Software, or Services in writing to TRITAN. Upon receipt of such requests, TRITAN shall issue a written Order for the work, each of which shall include the Solutions, Software or Services requested as well as the terms, requirements, and associated Fees for the requested Solutions, Software or Services.

(b) The Parties will endeavor to agree upon the terms for such Order and execute the Order within thirty (30) days of the date from which TRITAN provides the Order to Client. Unless mutually extended by the Parties, any Order not signed within thirty (30) days shall be void. If an Order is rejected, all other existing Orders and this Enterprise Agreement shall continue in full force and effect without the work covered by the Order.

4.2 Change Management

(a) Change Request Procedure. Either Party ("**Requester**") may request changes to an Order by submitting to the other Party ("**Recipient**") a written description of the requested change ("**Change Request**"). The Change Request shall contain sufficient detail for the Recipient to analyze and assess the change. Within fifteen (15) business days of receipt of a written Change Request, the Recipient will provide a written response to the Requester indicating the Recipients acceptance of, modification to, or rejection of the Change Request.

(b) All Change Requests are subject to approval in writing by both Parties and may require either a new Order or an amendment to an existing Order, depending on the scope of the changes.

4.3 Changes to Standards and Policies. Changes to standards, policies, practices, procedures or controls to be utilized by the Parties will be made in accordance with established Change Management processes and shall be delivered and acknowledged in writing as set forth in this Enterprise Agreement. Notwithstanding the forgoing, the Parties will not request changes that would be reasonably expected to (a) adversely impact the Solutions in a material manner or (b) compromise the security of Client's data.

5.0 TERM AND TERMINATION

5.1 Term. The initial term of this Enterprise Agreement begins on the Effective Date and, unless terminated earlier pursuant to any provision of this Enterprise Agreement, will continue in effect for five (5) years (the "**Initial Term**"). This Enterprise Agreement will automatically renew for additional, successive two (2) year terms unless either Party gives the other Party written notice of non-renewal at least ninety (90) days prior to the expiration of the then-current term (each a "**Renewal Term**" and together with the Initial Term, the "**Term**"). Client and TRITAN shall use reasonable best efforts to extend the Term, when applicable.

5.2 Termination of Agreement. In addition to any other express termination right set forth in this Enterprise Agreement:

(a) TRITAN may terminate this Enterprise Agreement, including any then active Orders, effective on written notice to Client, if Client fails to pay any amount when due hereunder, and such failure continues more than twenty (20) business days after TRITAN's delivery of written notice thereof to Client;

(b) Either Party may terminate this Enterprise Agreement, including any then active Orders, effective on written notice to the other Party, if the other Party materially breaches this Enterprise Agreement, and such breach: (i) is incapable of cure; or (ii) being capable of cure, remains uncured sixty (60) days after the non-breaching Party provides the breaching Party with written notice of such breach; or

(c) Either Party may terminate this Enterprise Agreement, including any then active Orders, effective immediately upon written notice to the other Party, if the other Party: (i) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (ii) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law; (iii) makes or seeks to make a general assignment for the benefit of its creditors; or (iv) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

5.3 Extending Cure Periods. Consent to extend a cure period under this Section shall not be unreasonably withheld by either Party, so long as the breaching Party has commenced good faith efforts to cure the breach during the sixty (60) day notice period.

5.4 Effect of Termination. In the event of expiration or termination of this Enterprise Agreement or one or more Orders for any reason, the duties and obligations of the Parties to each other shall end, other than (a) those duties and obligations which accrued prior to the date of expiration or termination hereof; (b) those terms of this Enterprise Agreement or the applicable Orders which, by their nature, extend beyond expiration or termination; (c) TRITAN's obligation to refund Client a prorated portion for any and all prepaid fees, including any Software or Service not accepted by the Client; and (d) Client's obligation to pay any outstanding amounts due to TRITAN, unless subject of a bona fide dispute. Neither Party shall be liable to the other for damages of any sort resulting solely

from terminating the Enterprise Agreement under its terms. Except as provided in Section 5.5 of these General Terms, in which case the provisions of this Section shall apply immediately upon expiration or termination of the Data Transition Period, upon termination of this Enterprise Agreement, Client shall immediately cease all use of the Software, Documentation, and other TRITAN Confidential Information, and shall delete and/or return all such items to TRITAN.

5.5 Transfer & Return of Data. Upon termination of this Enterprise Agreement, TRITAN shall return to Client all Client data in TRITAN's possession or control, and shall, upon request, provide all reasonable cooperation to transfer Client data to Client or a vendor that replaces TRITAN for Client (the "**Data Transition"**). TRITAN's obligations under this Section are conditioned on; (a) TRITAN receiving written request from Client to implement this Section; and (b) Client paying TRITAN in full for any Software provided or Service rendered during the Term, unless subject of a bona fide dispute, and (c) Client paying TRITAN, at the Professional Services rates set forth in <<***Payment Terms>>***, for its efforts to assist in such Data Transition. To facilitate the Data Transition, TRITAN shall provide all data, where applicable, in the following formats; (a) an established ANSI-approved standard or applicable protocol; (b) PDF format for scanned documents; and (c) .JPEG format for stored images, unless an alternate format has been agreed to in writing by both Parties. Upon a Termination, TRITAN shall provide Services under this Section (the "**Data Transition Period**") until the earlier of (a) written notice of completion and receipt of data by the Client or; (b) one hundred and twenty (120) days from the date of Termination of the Enterprise Agreement which will effectively end the Data Transition Period. If a termination is due to a breach by either Party, the other Party agrees that the Breaching Party will not be deemed in continuing breach during the Data Transition Period described in this Section. TRITAN shall provide transition services to Client, if requested, that include, without limitation, de-installation of the Software; off-hours support; assistance in aiding a new vendor by answering questions; and such other services as are reasonably requested. TRITAN shall be paid its standard hourly rates for providing transition services. If necessary, Client may continue use of the Software and Services as required to assist with a transition if Client pays for any additional use and demonstrates good faith in its transition efforts.

5.6 Survival. All provisions of this Enterprise Agreement which by their terms are anticipated to survive the expiration or termination of this Enterprise Agreement shall survive such expiration or termination until fully performed.

6.0 CONFIDENTIAL INFORMATION.

6.1 Confidential Information. In connection with this Enterprise Agreement each Party (as the "**Disclosing Party**") may disclose or make available Confidential Information to the other Party (as the "**Receiving Party**"). "**Confidential Information**" means information in any form or medium (whether oral, written, electronic, or other) that the Disclosing Party considers confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations.

6.2 Exclusions. Confidential Information does not include information that the Receiving Party can demonstrate by written or other documentary records: (a) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Enterprise Agreement; (b) was or becomes generally known by the public other than by the Receiving Party's or any of its Representatives' noncompliance with this Enterprise Agreement; (c) was or is received by the Receiving Party on a non-confidential basis from a third-party that was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; or (d) was or is independently developed by the Receiving Party without reference to or use of any Confidential Information.

6.3 Protection of Confidential Information. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party shall:

(a) not access or use Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Enterprise Agreement;

(b) except as may be permitted by this Enterprise Agreement, not disclose or permit access to Confidential Information other than to its Representatives who: (i) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Enterprise Agreement; (ii) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Section; and (iii) are bound by confidentiality and restricted use obligations with the Receiving Party or its Subcontractors that are at least as protective of the Confidential Information as the terms set forth in this Section;

(c) safeguard the Confidential Information from unauthorized use, access, or disclosure using at least the degree of care it uses to protect its most sensitive information and in no event less than a reasonable degree of care; and

(d) promptly notify the Disclosing Party of any unauthorized use or disclosure of Confidential Information and cooperate with Disclosing Party to prevent further unauthorized use or disclosure; and

(e) ensure its Representatives' compliance with, and be responsible and liable for any of its Representatives' non-compliance with, the terms of this Section.

6.4 Notwithstanding any other provisions of this Enterprise Agreement, the Receiving Party's obligations under this Section with respect to any Confidential Information that constitutes a trade secret under any applicable Law will continue until such time, if

ever, as such Confidential Information ceases to qualify for trade secret protection under one or more such applicable Laws other than as a result of any act or omission of the Receiving Party or any of its Representatives.

6.5 Compelled Disclosures. If the Receiving Party or any of its Representatives is compelled by applicable Law to disclose any Confidential Information then, to the extent permitted by applicable Law, the Receiving Party shall: (a) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can seek a protective order or other remedy or waive its rights under Section 6.3 of these General Terms; and (b) provide reasonable assistance to the Disclosing Party, at the Disclosing Party's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this Section, the Receiving Party remains required by Law to disclose any Confidential Information, the Receiving Party shall disclose only that portion of the Confidential Information that, on the advice of the Receiving Party's legal counsel, the Receiving Party is legally required to disclose and, shall use commercially reasonable efforts to obtain assurances from the applicable court or other presiding authority that such Confidential Information will be afforded confidential treatment.

7.0 INTELLECTUAL PROPERTY OWNERSHIP.

7.1 Software, Documentation, Deliverables. Client acknowledges that, as between Client and TRITAN, TRITAN owns all right, title, and interest, including all Intellectual Property Rights, in and to the Solutions, Software, Documentation, Services and Deliverables. Nothing in this Enterprise Agreement grants Client any right, title, interest or ownership to any of TRITAN's Intellectual Property Rights. For the avoidance of doubt, should Client request TRITAN develop a new feature or functionality for the Solutions, all rights in and to such new feature or functionality (including, but not limited to Deliverables) remain with TRITAN and TRITAN shall be free to use such feature or functionality as part of the Solutions, without any compensation to Client, even if Client requested the new feature or functionality.

7.2 Pre-existing Work.

(a) *By TRITAN*. TRITAN will continue to own all rights in any computer code or other materials developed or obtained outside of the scope of this Enterprise Agreement ("**Pre-existing Work**"). Notwithstanding anything to the contrary, Client shall have the right during the Term to access and use all Interfaces and other Deliverables created by TRITAN pursuant to the terms of this Enterprise Agreement.

(b) *By Client*. Client will continue to own all rights in any materials it developed or otherwise obtained outside of the scope of this Enterprise Agreement and that it owned and or created prior to execution hereof. Notwithstanding anything to the contrary, TRITAN shall, to the extent necessary, have the right during the Term to access and use all materials owned or licensed by Client that are necessary for TRITAN to perform its obligations under this Enterprise Agreement, subject to the terms and conditions of this Enterprise Agreement**.**

7.3 Retention. Client acknowledges that TRITAN provides similar Solutions, Software and Services to other Clients and that nothing in this Enterprise Agreement will be construed to prevent TRITAN from carrying on such business. Nothing in this Enterprise Agreement will allow Client to distribute, disclose or create derivative works of the Solutions, Software, the Documentation, the Services, the Deliverables, or TRITAN's Confidential Information as such term is defined in this Section.

8.0 REGULATORY ACCESS To the extent required by law, until (a) the expiration of two (2) years after the furnishing of any Services or Software pursuant to this Enterprise Agreement; or (b) such other time period mandated by any applicable law, rules or regulations, TRITAN will make available, upon the written request of a recognized government with presiding jurisdiction over TRITAN or Client, or any of their duly authorized representatives, copies of this Enterprise Agreement and any books, documents, records and other data of TRITAN that are necessary to certify the nature and extent of costs incurred by Client for such services. To the extent required by applicable law, TRITAN will cause any subcontractors to agree to the same requirements as set-forth immediately above.

9.0 SUBSTANCE OF COMMUNICATIONS TRITAN shall have no liability or responsibility for the substance of any communications transmitted by Client via the Solutions, and Client shall defend, indemnify and hold TRITAN harmless from any and all claims (including claims by governmental entities) related to such content and/or communications. TRITAN provides only access to the Software and Service; TRITAN does not operate or control the information, opinions or other substance created by Client or its Authorized Users, and TRITAN accepts no liability for such items.

10.0 NETWORK SECURITY To the extent that it is given access to Client systems in order to fulfill its obligations hereunder, TRITAN will be subject to Client's network security policy, which is as follows as of the date hereof (but subject to change upon prior notice to TRITAN). TRITAN will have access to Client systems through Client designated user-ids and passwords only. TRITAN shall notify Client immediately of user terminations or changes in job functions so that access privileges can be modified by Client accordingly. TRITAN is responsible for all use of and access to the Client network system by its employees and permitted subcontractors, and Client maintains the right to monitor all user activity and revoke access due to noncompliance to its security policies. It is agreed by TRITAN that the Client network security policy will only allow authorized users access and will deny all unauthorized access. TRITAN servers are protected by an industry standard firewall. Additionally, the security policy mandates presence of industry standard

Antivirus software on every desktop. To the extent Client requires TRITAN to implement different firewall or antivirus software for the Services, TRITAN will implement the same, upon mutual agreement between Client and TRITAN for the additional cost. TRITAN will perform any upgrades required, if and when required for the applicable Services being provided. TRITAN must notify Client immediately upon its knowledge of any security breaches including, but not limited to, unauthorized access and virus infections. TRITAN will permit Client to do the same. In case there is any non-compliance of the terms hereof, the same will be rectified by TRITAN at TRITAN's cost.

11.0 AUDIT TRITAN shall keep accurate and complete records of all matters relevant to or as required by this Enterprise Agreement. Client or its duly authorized representative shall have continuing access to inspect TRITAN's relevant books and records at any reasonable time or times upon prior notice to TRITAN in order: (a) to verify the amounts invoiced by TRITAN hereunder; and (b) to insure compliance by TRITAN with its obligations hereunder. If any inspection reveals an overpayment by Client TRITAN shall promptly reimburse to Client, the overpayment amount. Client's rights referred to above shall be exercised at the discretion of Client

12.0 INSURANCE TRITAN agrees to obtain and maintain, at its own expense: (a) Worker's Compensation/ Employer's Liability insurance covering its employees; (b) Commercial General Liability insurance including contractual liability and for bodily injury and property damage for at least $1,000,000 on a per occurrence basis covering claims arising out of or in connection with TRITAN's operations or the actions of its employees and independent contractors. Said policy shall also cover liability arising from doing business on the web including coverage for corruption and loss or theft of data. The insurance coverage required shall be placed with insurance company or companies reasonably acceptable to Client and have a rating equivalent to a current A. M. Best Company guide of A- or better. Client shall be named as an additional insured party under each such insurance policy (with the exception of Worker's Compensation), any "other insurance clause" shall be deleted from each such policy, and the insurance under each such policy shall be primary. The policies will include an endorsement waiving the Insurer's right of recovery and subrogation against Client. TRITAN's insurance policies shall provide for 30 days written notice to Client from the insurer in the event of any modification, cancellation or termination. TRITAN shall furnish Client a certificate of insurance, evidencing the coverage described herein, upon written request by the Client.

13.0 LIMITED WARRANTIES AND WARRANTY DISCLAIMER

13.1 Software Warranty. Unless otherwise stated in an Order, TRITAN represents and warrants to Client that the Software will operate materially in accordance with its specifications and the terms of this Enterprise Agreement, for so long as TRITAN provides both Support Services (under <<**Support Terms>>**) and Hosting & Data Management (under <<**Hosting Terms>>**). Upon any expiration, termination or suspension of the Support Services and/or Hosting & Data Management, this warranty shall end, and thereafter TRITAN makes no warranties, disclaims and excludes all representations, warranties and conditions related to the Solutions. In the event of termination of this Enterprise Agreement or an Order due to defective Software under this Section, Client shall obtain a refund of monies paid for the defective Software, provided that; (a) the Software was not Accepted by Client, and (b) the Software is no longer in use by Client. If TRITAN repairs or replaces the Software, the warranty will continue to run from the Effective Date and not from Client's receipt of the repair or replacement. The remedies set forth in this Section shall be Client's sole remedies and TRITAN's sole liability under the warranties set forth herein.

13.2 Service(s) Warranty. TRITAN warrants to Client that the Services will be performed in accordance with their respective documentation and in a professional and workmanlike manner by experienced, trained individuals and in accordance with prevailing industry practices and standards that generally are applicable to such Services. TRITAN's sole obligation and Client's sole remedy in the event of breach of this warranty is that TRITAN will promptly re-perform any Service not in compliance with the above warranty, provided that Client notifies TRITAN in writing of such noncompliance within a reasonable time after the applicable Service is performed, not to exceed thirty (30) days. In the event TRITAN fails to remedy any material noncompliance after re-performing any Service, Client shall be entitled to implement the default and termination provisions of this Enterprise Agreement. In the event of termination of this Enterprise Agreement due to defective Services, Client shall obtain a refund of monies paid for the defective Services, provided that; (a) the Services were not accepted by Client, and (b) the Software is no longer in use by Client.

13.3 Exceptions. The warranties set forth in this Section. do not apply and become null and void if Client breaches any material provision of this Enterprise Agreement, or if Client, any Authorized User, or any other person provided access to the Software by Client or any Authorized User, whether or not in violation of this Enterprise Agreement: (a) installs or uses the Software or Services on or in connection with any hardware or software not specified for use with the Software or Services; (b) modifies or damages the Software; or (c) misuses the Software, including any use of the Software other than as specified in the this Enterprise Agreement, the Order or the Documentation.

13.4 Disclaimer. EXCEPT FOR THE LIMITED EXPRESS WARRANTIES SET FORTH IN THIS SECTION 13 OF THE GENERAL TERMS, THE SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND TRITAN HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. TRITAN SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUALITY AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, TRITAN MAKES NO WARRANTY OF ANY KIND THAT THE SOLUTIONS, SOFTWARE, SERVICES OR DOCUMENTATION, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CLIENT'S

OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE. TRITAN will not be liable for any services or products provided by third-party vendors, developers or consultants identified or referred to Client by TRITAN, except as provided by the third-party to TRITAN, which warranties shall be made available to Client hereunder.

14.0 INDEMNIFICATION

14.1 Mutual. Each Party (the "**Indemnifying Party**") shall defend, indemnify and hold harmless the other Party, and its officers, directors, employees, affiliates, successors and assigns (the "**Indemnified Parties**") from and against, any and all claims, liabilities, costs, damages and/or expenses of any kind including, without limitation, court costs and reasonable attorneys' fees, (collectively "**Losses**") asserted by third-parties and arising out of or in connection with any grossly negligent or willful acts or omissions of the Indemnifying Party or its employees, independent contractors and/or agents in violation of this Enterprise Agreement.

14.2 By TRITAN.

(a) *Indemnification*. TRITAN shall defend, indemnify, and hold harmless Client from and against any and all Losses incurred by Client and resulting from any third-party claim, suit, action or proceeding ("**Third-Party Claim**") (a) alleging that the Software or Services, or any use of the Software or Services in accordance with this Enterprise Agreement, infringe or misappropriate such third-party's US Intellectual Property Rights or (b) arising out of TRITAN's material breach of its obligations under this Enterprise Agreement.

(b) *Anticipated Claims*. If a Third Party Claim based on Intellectual Property Rights is made or appears possible, as determined in TRITAN's sole discretion, TRITAN shall have the right to (a) modify or replace the Software, Documentation, or any component or part thereof, to make it non-infringing while retaining as closely as possible the original functionality, or (b) obtain the right for Client to continue to use such Software, Documentation, or any component or part thereof. If TRITAN determines that neither of these alternatives is reasonably available, TRITAN may terminate this Enterprise Agreement, in its entirety or with respect to the affected component or part, effective immediately on written notice to Client.

(c) *Exceptions*. TRITAN will not have any indemnification obligations to the extent that the alleged infringement arises from: (a) use of the Software or Services other than as permitted and provided for in this Enterprise Agreement; (b) use of the Software or Services in combination with data, software, hardware, equipment, or technology not provided by TRITAN or authorized by TRITAN in writing; (c) modifications to the Software not made by TRITAN; (d) use of any version of the Software other than the most current version of the Software delivered to Client; or (e) third-party products or services.

(d) *Sole Remedy*. THIS SECTION 14.2 SETS FORTH CLIENT'S SOLE REMEDIES AND TRITAN'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED THIRD-PARTY CLAIMS THAT THE SOFTWARE OR SERVICES INFRINGE, MISAPPROPRIATE, OR OTHERWISE VIOLATE ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

14.3 By Client. Client shall defend, indemnify, and hold harmless TRITAN from and against any and all Losses incurred by TRITAN and resulting from any Third Party Claim based on Client's, or any Authorized User's: (a) use of the Software or Services other than as permitted or provided for in this Enterprise Agreement; (b) use of the Software or Services in combination with data, software, hardware, equipment or technology not provided by TRITAN or authorized by TRITAN in writing; (c) modifications to the Software not made by TRITAN; or (d) use of any version of the Software other than the most current version of the Software delivered to Client.

14.4 Procedures. To receive the foregoing indemnities, the Indemnified Party shall promptly notify the Indemnifying Party in writing of a claim or suit and provide reasonable cooperation (at the Indemnifying Party's expense) and grant the Indemnifying Party the sole and full authority to defend the claim or suit; provided, however, the Indemnified Party may participate in the defense of such claim or suit at its expense. The Indemnifying Party shall have no obligation to indemnify the Indemnified Party under any settlement made without the Indemnifying Party's written consent (which shall not be unreasonably withheld). Each Party will promptly communicate to the other any offer received by or proposed to be made in settlement of any claim, matter or action that is subject to indemnification under this Section 14.4, and each Party will promptly and reasonably consider any such settlement offer or proposal that the other Party desires to accept or make.

14.5 Settlements. The Indemnifying Party may not settle any Third-Party Claim against the Indemnified Party without consent unless such settlement completely and forever releases the Indemnified Party from all liability with respect to such Third-Party Claim or unless the Indemnified Party consents to such settlement.

15.0 LIMITATIONS OF LIABILITY

15.1 WAIVER. IN NO EVENT WILL TRITAN BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES; (b) INCREASED COSTS, DIMINUTION IN VALUE OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (c) LOSS OF GOODWILL OR REPUTATION; (d) USE, INABILITY TO USE, LOSS, INTERRUPTION, DELAY OR RECOVERY OF ANY DATA, OR BREACH OF DATA OR SYSTEM SECURITY; OR (e) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER TRITAN WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE.

15.2 MONETARY CAP. IN NO EVENT WILL TRITAN'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE EXCEED AN AMOUNT EQUAL TO THAT ACTUALLY PAID BY CLIENT TO TRITAN FOR THE SOFTWARE AND/OR SERVICES GIVING RISE TO THE CLAIM IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE ACT OR OMISSIONS GIVING RISE TO THE CLAIM, LESS ANY CREDITS RECEIVED BY CLIENT FROM TRITAN DURING THE SAME TIME PERIOD.

15.3 Exclusions. The limitations and exclusions set forth in Section 15.1 and 15.2 of these General Terms, do not apply to the extent any such damage or liability results from (a) the breach of any data protection obligations under the ***<<Data Processing Terms>>***; (b) the gross negligence or intentional tortuous conduct of a Party; (c) violation of TRITAN's Intellectual Property rights; (d) indemnification by a Party pursuant to Section 14 of these General Terms; or (e) obligations to pay Fees.

16.0 DISPUTE RESOLUTION

16.1 Escalation & Mediation. If a dispute arises between Client and TRITAN which cannot be resolved in the normal course, then either Party may activate the following dispute resolution procedures: The Parties' respective Project Executives shall meet to resolve the dispute. If they do not resolve the dispute within twenty (20) business days, the issue shall be escalated to the Governance Committee, which shall have thirty (30) days to resolve the dispute. If the dispute has not been resolved within that thirty (30) day period, the issue shall be resolved through mediation. The Parties agree to select a mutually agreeable, neutral third-party to serve as a mediator in accordance with the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure. The mediation will take place in Cork, Ireland and the language of the mediation shall be English. The Mediation Agreement referred to in the Model Mediation Procedure shall be governed and construed and take effect in accordance with the laws of Ireland. Except as may be required by law, neither a party nor the mediators may disclose the existence, content or results of any mediation without the prior written consent of both parties. The mediator will have no authority to award punitive damages, consequential damages, or liquidated damages, or any damages exceeding the limitations set forth in this Enterprise Agreement.

16.2 Costs and fees associated with the mediation shall be shared equally by the Parties. If the Parties are unable to agree upon a mediator, they will engage a professional mediation service to select a mediator. If the Parties are not able to resolve the matter through mediation within sixty (60) days of selection of a mediator, then the parties will submit the dispute to binding arbitration in accordance with the Arbitration Act 2010 of the Republic of Ireland.

Binding Arbitration

16.3 Right to Withhold Payment. In the ordinary course of business, the Parties may encounter disputes about invoices. In the event of a bona fide good faith dispute regarding an amount invoiced by TRITAN, Client may withhold payment, without penalty, provided that (a) Client provides prompt, detailed written notice of the dispute at least (5) five calendar days prior to the payment due date; (b) Client cooperates with TRITAN in the investigation and analysis of the dispute; (c) Client pays all undisputed amounts not directly related to the dispute in a timely manner; and (d) promptly upon resolution of the dispute, Client pays to TRITAN any remaining amounts due. In the event Client withholds payment in violation of this Section, or for any reason other than an invoice dispute, TRITAN shall have the right, without penalty, to charge Late Fees in accordance with the ***<<Payment Terms>>*** on any unpaid amounts, initiate its rights under this Section 16 of these General Terms and/or declare this Enterprise Agreement in default.

17.0 MISCELLANEOUS

17.1 Exclusivity. The Client agrees that during the term of this Enterprise Agreement, TRITAN shall be the exclusive vendor for the provision of the Software and Services provided pursuant to this Enterprise Agreement and Orders. All exclusivity shall cease on termination of the Enterprise Agreement.

17.2 Notices. All notices or communications permitted or required under this Enterprise Agreement ("**Notice**") must be in writing. Notice to TRITAN should be addressed to: Tritan Software International; PO Box 13197, South City DSU, Cork, IE T12 C825; Attn: Cristina Wallis; Phone: +1-305-699-5000, Ext. 8110; Email: cwallis@tritansoft.com. Notices to Client should be addressed to the name and address set forth in the Order. Either Party may update its address by written notice in accordance with this provision. All Notices must be delivered by personal delivery, nationally recognized overnight courier (with all fees pre-paid), or email (with confirmation of transmission and a copy sent via First Class Mail on the same day). Notices are effective upon confirmation of receipt or refusal of delivery by the receiving Party.

17.3 Force Majeure. In no event shall either Party be liable to the other Party, or be deemed to have breached this Enterprise Agreement, for any failure or delay in performing its obligations under this Enterprise Agreement, (except for any obligations to make payments), if and to the extent such failure or delay is caused by any circumstances beyond such Party's reasonable control, including but not limited to acts of God, flood, fire, earthquake, hurricane, explosion, war, terrorism, invasion, riot or other civil unrest, strikes (other than by a Party's employees), industrial disturbances, or passage of law or any action taken by a governmental or public authority that preclude the activities contemplated by this Enterprise Agreement. The Party so affected will give the other Party prompt and detailed notice of the Force Majeure, including the probable duration thereof, and will promptly notify the other Party when the Force Majeure has ended. During the Force Majeure, the affected Party will use commercially reasonable efforts to avoid,

reduce or eliminate the Force Majeure's prevention, restriction or delay of the performance of its obligations under this Enterprise Agreement. If a Force Majeure event exceeds thirty (30) calendar days, the other Party may terminate this Enterprise Agreement by providing written notice to the Party asserting Force Majeure.

17.4 No Inferences. The Parties acknowledge that this Enterprise Agreement has been fully negotiated by the Parties and their respective legal counsel. In the event of ambiguities in this Enterprise Agreement, no inferences shall be drawn against either Party on the basis of authorship of this Enterprise Agreement.

17.5 Amendment and Modification; Waiver. Any amendment to or modification of this Enterprise Agreement must be in writing and signed by an authorized representative of each Party. Any waiver of any provisions of this Enterprise Agreement or rights thereunder must be in writing and signed by the Party so waiving. Except as otherwise set forth in this Enterprise Agreement, (a) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Enterprise Agreement will operate or be construed as a waiver thereof and (b) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

17.6 Severability. If any provision of this Enterprise Agreement is invalid, illegal, or unenforceable in any jurisdiction, the Parties shall negotiate in good faith to modify this Enterprise Agreement so as to effect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible. If the Parties are unable to reach a mutually acceptable modification, such provisions shall be deemed severed from this Enterprise Agreement and the remainder of the Enterprise Agreement shall remain in full force and effect as if such invalid provision had been omitted.

17.7 Assignment. Client may not assign or transfer any of its rights or delegate any of its obligations hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, without the prior written consent of TRITAN, except that Client may assign or transfer to its Affiliates by providing written notice to TRITAN no less than thirty (30) days prior to the assignment or transfer. Any purported assignment, transfer, or delegation in violation of this Section is null and void. No assignment, transfer, or delegation by Client will relieve Client of any of its obligations hereunder. Subject to the foregoing restrictions, this Enterprise Agreement is binding upon and inures to the benefit of the Parties hereto and their respective permitted successors and assigns.

17.8 Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under the ***<<Data Processing Terms>>***, the Confidentiality Provision of these General Terms, and in the case of Client, the License Grant in the Enterprise Agreement and the ***<<License Terms>>***, would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other Party will be entitled to seek equitable relief, without the need to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

17.9 Counterparts. This Enterprise Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement.

17.10 Electronic Signatures. The Parties agree that any electronic versions of signatures, whether through electronic forms or the transmission of PDF versions of signatures by email or facsimile shall have the same force and effect as original signatures.

17.11 No Partnership or Joint Venture. Nothing herein contained shall constitute a partnership between or joint venture by the Parties hereto or constitute either Party the agent of the other. No Party shall hold itself out contrary to the terms of this Enterprise Agreement and no Party shall become liable by any representation, act or omission of the other contrary to the provisions hereof. This Enterprise Agreement is not for the benefit of and grants no rights or remedies to any third-party.

17.12 Anti-Bribery. The Parties represent, warrant and undertake to each other on a continuous basis that they shall comply with all applicable anti-bribery, anti-money laundering, anti-slavery and human trafficking laws, rules, and regulations of the UK, the European Union and any other applicable jurisdictions. These laws include, without limitation, the currently effective or successor versions of the UK Bribery Act 2010; the UK Anti-Terrorism, Crime and Security Act 2001; the UK Proceeds of Crime Act 2002; The UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and the UK Modern Slavery Act 2015. In addition, the Parties represent, warrant and undertake that they shall each respectively take no action which would subject the other Party to fines or penalties under such laws, regulations, rules or requirements. Without prejudice to the above provisions, neither Party shall, directly or indirectly, pay salaries, commissions or fees, or make payments or rebates to employees or officers of the other Party; or favor employees or officers of the other Party or their designees with gifts or entertainment of unreasonable cost or value or services or goods sold at less than full market value; or enter into business arrangements with employees or officers of the other Party unless such employees or officers are acting as representatives of the other Party.

17.13 Governing Law. This Enterprise Agreement is governed by and construed in accordance with the laws of the Republic of Ireland, without giving effect to any choice or conflict of law provision or rule. This Enterprise Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

17.14 Entire Agreement. This Enterprise Agreement, together with the Exhibits and any other documents incorporated herein by reference, constitutes the sole and entire agreement of the Parties with respect to the subject hereof and supersedes all prior and contemporaneous understandings and agreements, both written and oral, with respect to such subject matter. In the event of any inconsistency between this Enterprise Agreement, the related Exhibits, and any other documents incorporated herein by reference, this Enterprise Agreement shall govern, followed by the Exhibits and then by the other documents incorporated by reference.

<<LICENSE TERMS>>

1.0 USE AND USERS.

1.1 Authorized Users. Each Order will specify the number of Client Locations covered by this Enterprise Agreement. Client is responsible for ensuring compliance of its Authorized Users across all Client Locations.

1.2 Use Restrictions. Neither Client nor its Authorized Users shall use the Software for any purposes beyond the scope of the license granted in this Enterprise Agreement. Without limiting the foregoing, neither Client nor its Authorized Users shall at any time, directly or indirectly:

(a) copy, modify, or create derivative works of the Software, in whole or in part;

(b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available the Software to any third-parties;

(c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code or any underlying algorithms, user interface techniques or other concepts embodied in the Software, in whole or in part;

(d) tamper with, or attempt to circumvent or disable, any license key;

(e) use the Software or its output to create, modify, or simulate designs for third-parties or to develop or enhance any product that competes with any TRITAN product or service;

(f) use any of the Software's components, files, modules, content, or related licensed materials separately from the Software;

(g) disclose the results of any benchmarking of the Software (whether or not the results were obtained with assistance from TRITAN) to any third-party;

(h) use the Software in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that violates any applicable law; or

(i) use the Software in any situation in which the failure or malfunction of the Software could reasonably be expected to result in personal injury, death, or catastrophic loss.

1.3 Reservation of Rights. TRITAN reserves all rights not expressly granted to Client in this Enterprise Agreement. Except for the limited rights and licenses expressly granted under this Enterprise Agreement, nothing in this Enterprise Agreement grants, by implication, waiver, estoppel, or otherwise, to Client or any third-party any Intellectual Property Rights or other right, title, or interest in or to the Software.

2.0 CLIENT RESPONSIBILITIES. Client is responsible and liable for all uses of the Software and Documentation resulting from access to and use of the Software through credentials or equipment issued by TRITAN to Client or Client's Authorized Users, whether directly or indirectly, and whether such access or use is permitted by or in violation of this Enterprise Agreement. Without limiting the generality of the foregoing, Client is responsible for all acts and omissions of its Authorized Users, including, but not limited to, any act or omission by an Authorized User that constitutes a breach of this Enterprise Agreement. Client shall make all Authorized Users aware of this Enterprise Agreement's provisions as applicable to such Authorized User and shall cause Authorized Users to comply with such provisions.

3.0 ACCEPTANCE. Upon delivery of Software to Client, TRITAN will issue a Completion Notice to the Client. Client will then have twenty (20) business days ("**Acceptance Period**"), unless otherwise mutually agreed to in an Order, to notify TRITAN of any material, reproducible defect of the Software to conform to this Enterprise Agreement or the applicable Order ("**Defect**"). If Client notifies TRITAN of any Defect within the Acceptance Period, TRITAN will use reasonable efforts to correct such Defect at its own expense, whereupon it will issue to Client a new Completion Notice and a new Acceptance Period of ten (10) business days will commence. If TRITAN is unable to correct such Defect, Client will have the right to terminate the Order in accordance with Section 5 of the General Terms. If Client does not provide TRITAN with a written notice of any material Defect during the Acceptance Period; the Software shall be deemed to be "**Accepted**" by Client. TRITAN will not unreasonably deny any request by Client to extend the Acceptance Period for as many as thirty (30) days.

4.0 SOFTWARE VERIFICATION PROCESS.

4.1 Client Reporting. In addition to any other audit rights provided for in this Enterprise Agreement, upon reasonable notice of not less than thirty (30) days, and not more than once per contract year, Client agrees to create and provide to TRITAN and its auditors a certificate that Client's use of the Software is, upon knowledge and belief, substantially in compliance with the terms of this Enterprise Agreement and any applicable Orders.

4.2 TRITAN Verification. Upon reasonable notice of not less than ten (10) days, and not more than once per contract year, TRITAN may verify Client's compliance with this Enterprise Agreement and applicable Orders at all Client Locations and for all environments in which Client uses the Software. Such verification will be conducted in a manner that minimizes disruption to

Client's business, and may be conducted remotely, or on Client's premises, during normal business hours. TRITAN may use an independent auditor to assist with such verification, provided TRITAN has a written confidentiality agreement in place with such auditor.

4.3 Discrepancies. TRITAN will notify Client in writing if any such verification indicates that Client has used any Software in violation of this Enterprise Agreement or is otherwise not in compliance with this Enterprise Agreement or the applicable Order. In the event the verification indicates use of the Software in excess of the license(s) granted, TRITAN may invoice Client for, and Client agrees to promptly pay for, any excess use.

<<SUPPORT TERMS >>

5.0 Level 1 Support.

5.1 Client is responsible for providing all Level 1 Support, including coordinating all activities and personnel required for such efforts. Level 1 Support includes:

(a) Responding to Authorized User reports;

(b) Ruling out any local issues (e.g.: user training issues, desktop problems, network problems, etc.);

(c) Verifying that the incident is a Software issue;

(d) Resolving any routine Software user access and permissions issues; and

(e) Gathering sufficient information from the person reporting the problem to appropriately scope the case, including, but not limited to, identifying specific examples of the problem and confirming that the problem is reproducible and what steps are required to reproduce the problem.

5.2 Client will escalate and submit a support request (**"Support Request**") to TRITAN only for those issues that it cannot resolve through Level 1 Support and that it reasonably assumes to be caused by the Solution itself.

6.0 Level 2 Support.

6.1 TRITAN is responsible for providing Level 2 Support, including coordinating all activities and personnel required for such efforts. Level 2 Support includes:

(a) Problem Resolution Support. Problem Resolution Support principally involves identification of individual issues directly resulting from the Software which have been escalated to TRITAN as a Support Request. A Support Request, also known as an "ticket," is defined as a single support issue which is reasonably suspected to be caused by the Solution. A single Support Request is a problem that cannot be broken down into subordinate issues. If a problem consists of subordinate issues, each subordinate issue shall be considered as a separate Support Request. In connection with a Support Request, TRITAN will provide:

(i) Advanced level technical expertise and support for all items directly relating to the Solution provided by TRITAN;

(ii) Assistance to Client's Level 1 Support for troubleshooting issues and assignment of severity levels;

(iii) Maintenance of the appropriate response levels and communication required to inform and assist the Client;

(iv) Coordination support for the appropriate TRITAN technical and management resources to facilitate resolution or involve additional resources for Client Support Requests;

(v) Information gathering to appropriately communicate any issues improperly assigned or discovered to be a result of Client-side technology including, but not limited to, specific examples of the problem and reproduction steps.

(b) Account Management Support. TRITAN shall provide assistance with service delivery planning, resource facilitation, support planning, escalation management, support usage and planning reviews in addition to guidance regarding best practices for support of the Software.

(c) Remote Support. Support shall be provided by TRITAN via remote access to Client's computing environment and through telephone, videoconference or email methods. In certain situations, as part of responding to Client's Support Request, TRITAN may also provide Client with a modification to the commercially available Software code to address specific critical problems ("**Hotfix**"). Hotfixes are designed to be released and implemented quickly to address Client's specific problems, and while each Hotfix will receive reasonable testing given the circumstances, except as otherwise provided herein or in an Order, Hotfixes may not be fully regression tested by TRITAN and will not be subject to individual acceptance testing by Client or to standard warranties set forth in this Enterprise Agreement.

(d) Onsite Support. Client can request Onsite Support as an additional Service. Issues requiring Onsite Support, that are not caused by a Defect in the Solution, will be charged on an hourly basis as set forth in the***<< Payment Terms>>***

(e) , and will Include charges for reasonable travel and living expenses approved by Client in writing. Tasks performed as part of Onsite Support will vary depending on the situation, environment, and business impact of the issue, and will be mutually confirmed by the Parties before work is undertaken.

(f) Professional & Supplemental Services. Client may, at any time, request additional Professional and/or Supplemental Services provided by TRITAN. All Fees shall be provided to the Client at the rates outlined in the ***<<Payment Terms>>*** and subject to resource availability.

7.0 SERVICE LEVELS

7.1 Generally. The Client shall identify in writing and TRITAN shall acknowledge a designated Client employee and a designated alternate employee permitted to submit Support Requests and serve as the Client's system administrator ("**System Administrator**"). Support Requests may only be submitted by the System Administrator and any changes to the System Administrator must be immediately reported to TRITAN in writing.

7.2 Severity Levels & Response Times. TRITAN shall use its best efforts to adhere to the response times outlined in this Section. When submitting a Support Request, Client will specify the initial Severity Level for the issue in consultation with

TRITAN. Client may request a change in Severity Level at any time by providing an explanation of the need for a change, and TRITAN will not unreasonably deny such requests. TRITAN reserves the right to downgrade the Severity Level of any Support Request if Client is not able to provide adequate resources or responses to enable TRITAN to continue with problem resolution efforts in a timely manner. Response times, including TRITAN's and Client's responsibilities, are defined as follows:

Severity Level	Description	TRITAN Response Time	Expected Client Response
1	Catastrophic Business Impact: Production application down or major malfunction resulting in an inoperative condition for all or the majority of users. The Software is unusable. **Submission via telephone only.**	1st response in < 2 hours Continuous effort on a 24x7 basis. * Rapid escalation within TRITAN. Notification of TRITAN senior executives.	Notification of senior executives at Client site. Allocation of appropriate resources to sustain continuous effort on a 24x7 basis. Rapid access and response from change control authority.
2	Critical business impact: Critical loss of application functionality or performance resulting in high number of users unable to perform their normal functions with impractical or no workaround available. The Software is usable but severely limited. **Submission via telephone only.**	1st response < 6 hours Continuous effort on a 24x7 basis. * Notification of TRITAN senior managers.	Allocation of appropriate resources to sustain continuous effort on a 24x7 basis. Rapid access and response from change control authority. Management notification.
3	Moderate business impact: Moderate loss of application functionality or performance resulting in multiple users impacted in their normal functions, but practical workaround exists. The Software is usable but limited. **Submission via phone, email or web portal.**	1st response in < 2 business days. Effort during business hours only.** Allocation of appropriate resources to sustain continuous effort during business hours*.	Allocation of appropriate resources to sustain continuous effort during business hours. Access and response from change control authority within 8 business hours*.
4	Minimal business impact: Minor loss of application functionality or performance not significantly impacting users. The Software is usable but may have inconveniences. **Submission via phone, email or web portal.**	1st response < 5 business days Effort during business hours only.**	Allocation of appropriate resources to sustain continuous effort during business hours. Access and response from change control authority in accordance with normal procedures.

*Includes holidays and weekends.
**Business hours shall be defined as 9AM to 6PM Greenwich Mean Time (GMT), Monday through Friday, excluding Irish public holidays.

8.0 RESOLUTION ACTIVITIES. Client may be required to perform reasonable problem determination and resolution activities as requested by TRITAN. Problem determination and resolution activities may include performing network traces, capturing error messages, collecting configuration information, changing product configurations, installing new releases of Software or implementing new Services.

9.0 MAINTENANCE SERVICES. During the Term of this Enterprise Agreement, TRITAN shall provide the following Maintenance Services:

9.1 Routine performance enhancements designed to improve or maintain the operation of the Software;
9.2 Routine security enhancements designed to improve or maintain the security of the Software;
9.3 Changes required for the Software to continue operating in accordance with applicable laws and regulations;
9.4 Fixes (interim bug fixes) and releases (distribution of minor and major foundational releases) of the Software;
9.5 Updated documentation and release notes; and

9.6 All maintenance services further specified within applicable Orders.

10.0 SOFTWARE UPDATES. TRITAN may from time to time, but is not required to unless otherwise specified in this Enterprise Agreement or an Order, develop or implement Updates for features within the Software. TRITAN shall provide Updates to Client on the terms and conditions they are offered to similarly situated clients.

10.1 Prerequisites & Assumptions. The delivery of Support Services under these Support Terms is conditioned upon the following prerequisites and assumptions:

(a) TRITAN will provide Support Services only for the current version of the commercially released, generally available Software.

(b) All Support Services will be provided in the English language unless otherwise agreed to by TRITAN and Client in writing.

(c) TRITAN will be permitted to access Client's computing environment via remote internet connections (e.g. Secure VPN, etc.) to analyze and resolve problems. TRITAN personnel will access only those systems authorized by Client in writing and will not access those systems without Client's express consent. In order to utilize remote access, Client must maintain reasonable internet access and provide TRITAN with appropriate credentials, procedures and permission to access Client's environment.

(d) Additional prerequisites and assumptions applicable to all Software Clients may be set forth in an Order.

(e) Client agrees to work with TRITAN to plan for the foreseeable utilization of Support Services. Client will comply with TRITAN's process for submitting Support Requests which shall utilize TRITAN's support tracking software to facilitate submission and management of Client Support Requests.

(f) Client agrees to provide support directly to its Client Locations and Authorized User community and to develop sustainable support procedures.

(g) Client agrees to provide an internal escalation process to facilitate communication between Client's management and TRITAN as appropriate.

(h) Client agrees, where applicable, to provide reasonable office space, telephone and internet access, and access to Client's systems and diagnostic tools to TRITAN personnel that are required to be onsite.

11.0 SATISFACTION SURVEYS. Client agrees to make reasonable efforts to participate in Client satisfaction surveys that TRITAN may provide from time-to-time regarding the Solutions, Software and Services.

<<HOSTING TERMS>>

12.0 SCOPE OF SERVICE

12.1 Data Facilities. In order to store and secure all information, including, but not limited to Personal Information, collected, stored and processed as a result of the Solutions, TRITAN utilizes a global network of secure data centers owned and operated by contracted third-parties (the "**Data Facilities**"). The Data Facilities have each received International Organization for Standardization (ISO) and Occupational Health and Safety Management System (OHSAS) certifications. TRITAN will ensure that its Subcontractors contracted to provide the Data Facilities are required to ensure the Data Facilities reside on capable communication networks and be equipped in accordance with recognized industry standards regarding disaster resistance and recovery capabilities. TRITAN will require all such Subcontractors to ensure the Data Facilities are protected and manned by security personnel on a twenty-four (24) hour, seven (7) days a week basis. TRITAN reserves the right to choose and change its Data Services Subcontractors at any time in its sole discretion.

12.2 Client-Provided Technology. TRITAN does not have any obligations, and accepts no liability, for the configuration, management, performance or any other issue relating to Client's routers, networks, servers, or other Client-provided technology used for access to or the exchange of data in connection with the Solutions, for which Client shall have the sole responsibility and liability.

12.3 Software. TRITAN will install only the Software and any technology required to operate the Software. TRITAN will not install nor be responsible for any Client-provided software. Any proprietary TRITAN technology installed by TRITAN, as required to run the Software, will remain the exclusive property of TRITAN.

12.4 Scheduled Maintenance. Scheduled maintenance for the Data Services will not normally result in service interruption or outage. However, in the event scheduled maintenance should require a service interruption or outage, TRITAN will: (a) use all reasonable efforts to provide Client with at least five (5) business days' prior notice of such scheduled maintenance; (b) cooperate with Client to minimize any disruption in the Data Services that may be caused by such scheduled maintenance; and (c) perform such scheduled maintenance during non-peak hours agreeable to both Parties. In no event shall such service interruption exceed eight (8) continuous business hours, excluding any unforeseen connectivity or Client network issues that are beyond TRITAN's ability to control.

12.5 Change Control. Changes to production environment(s) will be made in accordance with established change control processes which shall be agreed upon by both Parties.

12.6 Monitoring. TRITAN will monitor the Solutions on a twenty-four (24) hour per day, seven (7) days per week basis, including monitoring the platform (servers, storage, data center and network components), as well as the Software. TRITAN will use all reasonable efforts to resolve issues that impact the Solutions identified through monitoring in accordance with the required service levels.

12.7 Data Interfaces & Network. Client is responsible to resolve any Off-Net related issues regarding interfaces or networks that are affecting the Solutions. When TRITAN identifies issues through monitoring that are the result of a problem with any Off-Net component, TRITAN will escalate said issues to the Client. The Client will provide a standard contact and escalation method for TRITAN to follow in such events. The Client will be solely responsible for coordinating its internal or third-party resources to work with TRITAN to resolve any such issues.

SERVICE LEVEL AVAILABILITY. TRITAN shall use its best efforts to ensure that the Solutions, through the provision of Data Services, remains available ninety-eight percent (98%) of each month ("**Service Level Availability**") per License for all On-Net Services within TRITAN Network. TRITAN's sole liability, and Client's sole remedy for TRITAN's failure to meet the Service Level Availability, shall be limited to Client's right to receive credit set forth in the table below. The credit specified in this table will be applied to the next scheduled Hosting and Data Management Fees reducing the amount owed for such Fees. TRITAN will not make cash refunds to Client as a result of Service Credit Availability will be measured and reported by TRITAN upon request from the Client. Measurement will be taken On-Net using a TRITAN utility that automatically retrieves and reports Software availability information available for the Client.

Availability	Credit
90-98%	10%
80-89%	20%
70-79%	30%

<70%	50%

For the purpose of determining Service Level Availability, the following formula will be used:

$$\text{Uptime Percentage} = \frac{\text{(Possible Available Uptime*)} - \text{(Hours of downtime)}}{\text{(Total Hours in the Month)}} * 100$$

* Possible Available Uptime will be calculated as: number of calendar days in a month times 24 hours, minus any Excused Outage during the calendar month, and Total Hours in the Month will be determined as the number of calendar days in a month times 24 hours.

13.0 SECURITY TRITAN shall periodically audit the security of the Software and Data Facilities applicable to the Client. This audit: (a) shall be performed periodically by TRITAN; (b) shall be performed according to appropriate industry security standards as elected by TRITAN; (c) shall be performed by third-party security professionals at TRITAN's election and expense; (d) shall result in the generation of an audit report ("**Security Audit Report**"); and (e) may be performed for other purposes in addition to satisfying this Section (e.g., as part of TRITAN's regular internal security procedures or to satisfy other contractual obligations). Upon written request by the Client, TRITAN shall provide, on a restricted and confidential basis, a redacted version of the Security Audit Report so that Client can reasonably verify TRITAN's compliance with its security obligations under this Enterprise Agreement. TRITAN may remove any information from the Security Audit Report or any other documentation or report that may compromise the security of TRITAN's technology environment or the confidentiality of any Confidential Information, provided that such removal does not prevent Client from understanding the substance of the Security Audit Report or other documentation or report. TRITAN shall make good faith, commercially reasonable efforts to remediate (1) any errors, identified in a Security Audit Report that could reasonably be expected to have an adverse impact on Client's use of the Solutions or protection and security of Client data, and (2) material control deficiencies identified in the Security Audit Report.

<<DATA PROCESSING TERMS>>

14.0 MUTUAL OBLIGATIONS The Client and TRITAN shall comply with their respective obligations under all applicable Data Privacy Laws and shall perform their respective obligations under this Enterprise Agreement in such a manner so as not to cause the other to be in breach of its obligations under the applicable Data Privacy Laws. The Client and TRITAN shall each be responsible for requiring any Subcontractor working on its behalf to fully comply with all Data Protection Laws and to perform the Subcontractor's obligations in a manner so as not to cause either Party to be in breach of its obligations under this Enterprise Agreement or the Data Privacy Laws.

15.0 CLIENT OBLIGATIONS

15.1 Consents & Reporting. The Client shall be responsible for any obligations to inform regulatory authorities or Individuals about the collection, processing or use of its, his or her Personal Data, including, but not limited to, (a) obtaining any necessary consents, releases, opt-ins, or opt-outs from all Individuals whose information will be entered into one or more Solutions, and (b) providing any breach notification requirements under the Data Privacy Laws. When requested by Client, TRITAN shall provide Client with any data necessary for Client to make determinations regarding reporting requirements, and Client shall reimburse TRITAN for the costs associated with such assistance at the rates for professional services outlined in these Terms and Conditions.

15.2 Client Responsibility. Client will defend, indemnify and hold harmless, TRITAN, from and against any and all claims, demands, causes of action, losses, costs or expenses, incurred by TRITAN as a result of Client's failure, or the failure of any of Client's Affiliates, or their respective Subcontractors or Authorized Users, to comply with Section 2.1 of these Data Processing Terms.

16.0 TRITAN OBLIGATIONS

16.1 TRITAN agrees that, in processing any Personal Data in the course of providing Solutions, TRITAN shall:

(a) not disclose any Personal Data to anyone other than to those of its personnel who reasonably require the same in order for TRITAN to perform its obligations under this Enterprise Agreement and the Order;

(b) assist the Client as reasonably necessary to enable the Client to comply with the applicable Data Privacy Laws;

(c) if required, establish a data protection official, and notify the Client of the name and contact information for such official; and

(d) if requested by the Client, enter into direct agreements with each of the Client's affiliates in a form acceptable to the Client to enable the Client and its Affiliates to comply with local data processing laws and requirements, including but not limited to agreements according to the ***<<Standard Contractual Clauses>>***.

16.2 Notwithstanding anything else in these Data Processing Terms, TRITAN shall not disclose Personal Data to a third-party or use such Personal Data for any purpose other than the performance of the Services. TRITAN shall use reasonable efforts to ensure (a) that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, and (b) the transport or storage of Personal Data on transmission facilities can be established and verified. TRITAN will have no liability for the actions or inactions of any third-parties engaged by the Client.

16.3 TRITAN will establish an audit trail to document whether and by whom Personal Data has been entered into, modified in, or removed from the Personal Data processing portions of the Software by TRITAN, and will ensure that Personal Data collected for different purposes is segregated and processed separately and only for its designated purpose.

16.4 TRITAN represents that as of the Effective Date, TRITAN is not under any obligation to disclose or otherwise make available Personal Data of the Client to any third-parties. This confirmation shall not apply to any statutory obligations to disclose such information (e.g. to an exchange supervisory authority, regulatory authority or fiscal authority), unless such obligations concern the disclosure to a government entity, an intelligence service or security authority having authority to require such disclosure. Unless prohibited by applicable law, TRITAN will immediately notify Client in writing if it is no longer able to comply with the provisions of these Data Processing Terms. The absence of an obligation to disclose or make available Personal Data does not limit TRITAN's right to engage Subcontractor's to whom Personal Data of the Client may be disclosed in order to facilitate provision of the Solutions; however, TRITAN will have a written agreement in place with such Subcontractors, pursuant to the terms of this Enterprise Agreement.

16.5 TRITAN shall ensure that any of TRITAN's personnel entrusted with processing the Personal Data have been duly instructed on the protective regulations of the Data Privacy Laws and the requirements of these Data Processing Terms.

16.6 TRITAN shall, without undue delay, inform Client in the case of a serious interruption of operations or violations by TRITAN of provisions to protect Personal Data or of terms specified in this Enterprise Agreement. In such an event, TRITAN shall implement the measures necessary to secure the Personal Data and to mitigate potential negative effects on the data subjects and shall agree upon the same with the Client without under delay.

16.7 If a data subject submits a request to TRITAN to correct, delete or block its, his or her Personal Data, TRITAN shall refer all such requests to the Client, and TRITAN shall not act on such requests without Client's instructions, except to inform the Data Subject that the inquiry has been forwarded to Client.

17.0 EU CLIENTS

Client shall indicate in the Order if it is required to comply with the GDPR. If so, the additional data processing terms, ***<<GDPR Processing Terms>>***, shall apply to this Enterprise Agreement.

18.0 HOSTING

Unless the ***<<GDPR Processing Terms>>*** apply or the Parties agree otherwise in writing, any hosting or other form of data storage performed by TRITAN, shall be carried out within a Data Facility location to be determined at TRITAN's sole discretion in order to adequately provision the Solutions. Upon request by the Client at any time, TRITAN will provide Client with a complete list of the facilities used by TRITAN for hosting the Personal Data in the course of providing the Solutions.

19.0 RETURN OF DATA Client reserves the right upon termination of the Enterprise Agreement that any Personal Data processed by TRITAN on behalf of the Client according to these Data Processing Terms that remains in the possession of or under the control of TRITAN is fully returned to the Client or deleted, and such transfer shall be handled as provided for in Section 5.5 of the General Terms.

<<GDPR PROCESSING TERMS>>

20.0 REMOTE PROCESSING

20.1 Authorization. TRITAN may, and Client hereby authorizes TRITAN to, carry out the Services from facilities of TRITAN or its agents located outside of the European Union, primarily within the United States (such activities hereinafter "**Remote Access**"). TRITAN will maintain the EU-US Privacy Shield Certification administered under the United States of America (US) Department of Commerce to ensure an adequate data transfer mechanism as defined under Article 45 of the EU GDPR, and TRITAN will perform Remote Access of Client Data for the explicit purposes of the provision of Services and obligations outlined within this Enterprise Agreement and associated Orders.

20.2 Maintenance. When performing any services required by this Enterprise Agreement by Remote Access, such access must not compromise the technical-organizational security measures agreed to in Annex B to the **<<SCCs>>**. TRITAN's personnel carrying out such activities must, to the extent possible, be physically located in TRITAN facilities where the technical-organizational security measures agreed to in Annex B to the **<<SCCs>>** are in place. Should Remote Access for maintenance be necessary, the Remote Access may only be carried out via encrypted, secure remote protocols designed to ensure that no Personal Data can be permanently copied to the equipment used by TRITAN's personnel during the Remote Access.

20.3 No Data Remains Outside the European Union. The technical-organizational security measures apply to any facilities from which Remote Access is carried out. TRITAN will use its best efforts to ensure that, after any Remote Access has been carried out, no personal data of the Client will remain or reside outside of the European Union. TRITAN will utilize subprocessors meeting the requirements of these GDPR Terms for the purpose of maintaining the Data Facilities for the provision of Services as it pertains to the data hosting obligations outlined within this Enterprise Agreement and applicable Orders. At any time, upon Client's request, TRITAN will provide Client the name of TRITAN's then current Subcontractor performing subprocessing obligations.

20.4 Revocation/Cancelation. The Client may cancel TRITAN's right to Remote Access and/or demand the Services are rendered via a European Union legal entity, in the event:

(a) the SCCs are revoked or withdrawn or otherwise become invalid;

(b) the GDPR Terms of the Enterprise Agreement and the SCCs are held by a court of competent jurisdiction to be invalid or to be an insufficient basis for cross-border data transfers;

(c) Client is requested by a Data Protection Authority, court or other competent official entity to stop the Remote Access, and/or

(d) Remote Access pursuant to these GDPR Terms is no longer compliant with applicable GDPR.

21.0 STANDARD CONTRACTUAL CLAUSES

21.1 SCCs. The Standard Contractual Clauses set forth at www.Tritansoft.com/standard_contractual_clauses ("**SCCs**"), will apply to the processing of Client's Data by TRITAN under this Enterprise Agreement. Upon execution of this Enterprise Agreement, TRITAN and the Client each are agreeing to the SCCs and all appendices attached thereto. The SCCs apply only to Personal Data that is transferred directly from the European Union to a location outside the European Union, whether directly or via a subsequent transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data, and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

21.2 Violation of SCCs. TRITAN and the EU Client agree that if either Party is held liable for a violation of the SCCs committed by the other Party, the violating Party will, to the extent to which it is liable, defend, indemnify and hold harmless the non-violating Party, from and against any claims, causes of action, costs, charges, damages, expenses or losses the other parties incurred as a result of the violating Party's violation of the SCCs.

Hierarchy Of Agreements. The SCCs shall have precedence over any other agreement relating to the Solutions, including this Enterprise Agreement and any Orders.

<<PAYMENT TERMS>>

22.0 PAYMENT TERMS

22.1 Payments Due. All invoices are due and payable net thirty (30) days from the date of the invoice, unless Client provides TRITAN with written notice of a dispute related to a charge on the invoice, in which case all undisputed portions of the invoice remain due and payable in accordance with these Payment Terms. All payments shall be made in U.S. dollars and are non-refundable.

22.2 Late Fees. If Client fails to make any payment when due, in addition to all other remedies that may be available: (i) TRITAN may charge interest on the past due amount at the rate of 2.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law; (ii) TRITAN may initiate its rights under the General Terms, Dispute Resolution Provisions and/or declare this Enterprise Agreement in default under the General Terms, Default Provisions. (iii) Client shall reimburse TRITAN for all costs incurred by TRITAN in collecting any late payments or interest, including attorneys' fees, court costs, and collection agency fees; and (iv) if such payment failure continues for thirty (30) days following written notice to Client of such failure, TRITAN may restrict Client and Client's Authorized Users' access to the Solutions until all past due amounts and interest thereon have been paid. TRITAN will have no liability to Client for any damages or costs associated with such restricted access to the Solutions, and the right to restrict access shall be in addition to any other remedies available to TRITAN under this Enterprise Agreement or the applicable Order. Client shall indemnify and hold TRITAN and its shareholders, officers, subsidiaries and affiliates harmless from and against all claims, costs, damages, and expenses, and reasonable attorneys' fees arising out of, directly or indirectly, such restricted access to the Solutions.

22.3 Taxes & Tariffs. All prices and payments in this Enterprise Agreement are exclusive of all taxes and similar assessments, and Client agrees to pay all national, international, state and local sales, use, value added, withholding and other taxes, customs duties and similar tariffs and fees based on the Solutions, Software and Services provided hereunder, other than taxes imposed on TRITAN's net income.

SOFTWARE LICENSE FEES The Software License Fees shall be payable to TRITAN by Client in accordance with the amounts outlined within the respective Order and the following payment schedule:

Description	Percentage Paid
Upon Execution of an Order	50% of Software License Fees
Upon Installation of the Software	Remaining 50% of Software License Fees

23.0 SUPPORT & MAINTENANCE The Support and Maintenance Fees shall be payable to TRITAN by Client and invoiced in accordance with the amounts outlined within the respective Order. Upon Installation of the Solutions, Support and Maintenance Fees are due and payable per Client Location and shall be prorated in accordance with the remaining days of the calendar year following Installation. Thereafter, Support and Maintenance Fees shall be payable annually and are due on the first day of each calendar year.

24.0 DATA MANAGEMENT & HOSTING FEES The Hosting & Data Management Fees shall be payable to TRITAN by Client and invoiced in accordance with the amounts outlined within the respective Order. Upon Installation of the Software, Hosting and Data Management Fees are due and payable per Client Location and shall be prorated in accordance with the remaining days of the calendar year following Installation. Thereafter, Hosting and Data Management Fees shall be payable annually and due on the first day of each calendar year.

PROFESSIONAL SERVICE FEES All Professional Service Fees shall be payable to TRITAN by Client and invoiced in accordance with the amounts outlined within the respective Order and the following payment schedule:

Description	Percentage Paid
Upon Execution of an Order for Addition of Professional Service(s)	50% of Professional Service Fees
Upon Completion of Professional Service(s)	Remaining 50% of Professional Service Fee

Professional Services shall be invoiced at the following rates and payment schedule:

Description	Rate/Hour
Project Management	Client- $150

Remote Training	Client- $150
*On-Site Training**	Client- $200
User Acceptance Testing & QA	Client- $200
Product Configuration	Client- $225
Technical Acceptance Testing & QA	Client- $225
Remote Hardware Technician/ Engineer	Client- $225
*On-Site Hardware Technician/ Engineer**	Client- $275
Programming Development	Client- $250

***Does not Include Travel and Expenses which are to be approved by both Parties in writing and paid by Client in accordance with this Enterprise Agreement.*

25.0 **RATE INCREASE LIMITATION** All Fees (including licensing Fees, Support and Maintenance Fees, Hosting & Data Management Fees, Professional Service Fees and Supplemental Service Fees) may not be increased more than once during each calendar year by an amount equal to the lesser of 3.5% or the percentage change in the U.S. Dept. of Labor, Consumer Price Index, All Urban Consumers ("**CPI**") as compared to the CPI one year earlier.

26.0 **TRAVEL & EXPENSES** Client will reimburse TRITAN for all travel and out of pocket expenses incurred in conjunction with providing the Software and Services, with such travel expenses to be charged in accordance with Client's travel policy. All other expenses will be billed to Client at cost.

<<DEFINITIONS>>

27.0 DEFINITIONS. In addition to capitalized terms defined elsewhere in this Enterprise Agreement, the following capitalized terms shall have the meanings set forth here.

27.1 "**Affiliate**" of a Party means, an entity that controls, is controlled by, or is under common control with the Party.

27.2 "**Authorized User**" means an employee or contractor of Client who Client permits to access and use the Software and Services pursuant to Client's license hereunder.

27.3 "**Completion Notice**" means a written notice from TRITAN stating that the Solutions, Software or Service ordered has been delivered or completed by TRITAN pursuant to terms of the applicable Order and is available for Client's use or testing.

27.4 "**Client**" means the entity identified on an Order as the Client as well as well as its Affiliates that elect to participate in this Enterprise Agreement as set forth herein.

27.5 "**Client Locations**" means the location or locations owned, operated, managed, contracted and/or occupied by Client, its Affiliates, or its Authorized Users to which the Solutions, Software or Services are delivered, including but not limited to or leased by TRITAN and used to deliver the Solutions, including terminals and other equipment, wires, lines, ports, routers, switches, channel service units, data service units, cabinets, racks, private rooms and the like.

27.6 "**Intellectual Property Rights**" means all right, title, and interest of every kind and nature whatsoever in and to any materials, including, but not limited to, Deliverables, developed by TRITAN (including without limitation any ideas, inventions, designs, improvements, discoveries, innovations, patents, trademarks, service marks, trade dress, trade names, trade secrets, works of authorship, copyrights, films, audio and video tapes, other audio and visual works of any kind, scripts, sketches, models, formulas, tests, analyses, software, firmware, computer processes and other applications, creations, properties, and any documentation or other memorialization containing or relating to the foregoing discovered Client vessels, shoreside Facilities, third-party operated locations and/or other locations as specified in writing by Client.

27.7 "**Data Privacy Laws**" means the data protection and privacy laws of all applicable countries and states, including, but not limited to, the EU General Data Protection Regulation.

27.8 "**Deliverable(s)**" means any Software, Service, item, task or activity that TRITAN is to provide as agreed to by both Parties and specified in an Order.

27.9 "**Documentation**" means TRITAN's user manuals, handbooks, and installation guides relating to the Solution provided by TRITAN to Client, either electronically or in hard copy form.

27.10 "**Excused Outage**" means any outage, unavailability, delay or other degradation of access to the Solutions related to, associated with or caused by scheduled maintenance or caused by circumstances beyond the control of Client or TRITAN.

27.11 "**Facilities**" means any property owned, invented, created, written, developed, taped, filmed, furnished, produced, or disclosed) in the course of providing the Solutions within the scope of this Enterprise Agreement.

27.12 "**Installation**" means the date on which the Software has been installed or is accessible at a Client Location and may be used to process data according to the specifications contained in the applicable Order.

27.13 "**Off-Net**" means services that originates from and/or terminates to any location that is not on the TRITAN Network.

27.14 "**On-Net**" means Services that originate from and terminate to a location that is on the TRITAN Network.

27.15 "**Operational Data**" means information related to system, operations and peripheral information relevant to operation of the Software and the provision of Services but excludes Personal Data.

27.16 "**Personal Data**" means any data or information collected or used by the Software or as part of the Services that relates to an identified or identifiable natural person.

27.17 "**Service**" means any TRITAN service offered by TRITAN as set forth herein or agreed to in an Order. For purposes of clarity, "Service" may include, without limitation, any professional services provided by TRITAN to Client for a fee.

27.18 "**Software**" means any TRITAN proprietary software product owned, offered and/or supported by TRITAN or set forth herein or agreed to in an Order. For purposes of clarity, "Software" shall not include third-party software.

27.19 "**TRITAN Network**" means the physical and virtual, private technical network, owned or leased and managed by TRITAN within the private technology infrastructure environment, both physical and virtual, managed by TRITAN for provisioning the Software and Services as it solely pertains to and is accessed by Client through secure internet and satellite communication methods.

27.20 "**Updates**" means any improvements, enhancements, replacements, supplements, bug fixes, patches, or modifications to the Software that TRITAN generally makes available free of charge to all clients.

<<HIPAA BUSINESS ASSOCIATE AGREEMENT>>

THIS BUSINESS ASSOCIATE AGREEMENT ("BA Agreement") is effective as of the _____ day of _____, 20___ (the "Effective Date") by and between the person or entity listed as the covered entity on the signature page hereto ("Covered Entity") and Tritan Software International, Ltd. ("Business Associate")

WHEREAS, Covered Entity has determined that it is a covered entity under HIPAA or has components covered by HIPAA;

WHEREAS, Covered Entity has retained Business Associate to provide certain goods or services to Covered Entity (collectively, the "Services") and in doing so Business Associate creates, receives, maintains, or transmits PHI that is subject to protection under HIPAA; and

WHEREAS, under HIPAA, Business Associate is classified as the business associate of Covered Entity.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

I. **Definitions.** The terms used, but otherwise not defined, in this BA Agreement shall have the same meaning as those terms in HIPAA and/or the Enterprise Agreement.

A. "Enterprise Agreement" shall mean that certain Enterprise Software License and Services Agreement, by and between the Business Associate and the Covered Entity pursuant to which Business Associate provides certain goods and/or services to Covered Entity and creates, receives, maintains, or transmits PHI.

B. "Breach" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

C. "Designated Record Set" shall have the meaning set forth in 45 CFR § 164.501, including, without limitation, a group of records maintained by or for Covered Entity that consist of: (i) the medical records and billing records about individuals maintained by or for Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) records used, in whole or in part, by or for Covered Entity to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for Covered Entity.

D. "HIPAA" shall mean: (i) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164, and any subsequent amendments or modifications thereto, and (ii) the HITECH Act, and regulations promulgated thereunder, and any subsequent amendments or modifications thereto.

E. "HITECH Act" shall mean the provisions applicable to business associates under the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

F. "PHI" shall mean Protected Health Information which Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity in connection with the performance of Services by Business Associate for Covered Entity pursuant to the Enterprise Agreement.

G. "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, as may be amended, modified or superseded, from time to time.

H. "Protected Health Information" shall have the meaning set forth in 45 CFR § 160.103, including, without limitation, any information, whether oral, electronic or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

I. "Required by Law" shall have the meaning set forth in 45 CFR § 164.103, including, without limitation, a mandate contained in law that compels Covered Entity or Business Associate to make a use or disclosure of Protected Health Information and that is enforceable in a court of law.

J. "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

K. "Security Incident" shall have the meaning set forth in 45 CFR § 164.304, including without limitation, the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

L. "Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, as may be amended, modified or superseded from time to time.

M. "Unsecured PHI" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, Protected Health Information not secured through the use of encryption, destruction or other technologies and methodologies identified by the Secretary to render such information unusable, unreadable, or indecipherable to unauthorized persons.

II. Obligations of Business Associate.

A. Permitted Uses. Business Associate is permitted to use PHI in order to provide the Services pursuant to the Enterprise Agreement; provided, however, that Business Associate shall not use PHI in any manner that would constitute a violation of HIPAA if so used by Covered Entity. Business Associate may use PHI: (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) as Required by Law.

B. Permitted Disclosures. Business Associate is permitted to disclose PHI in order to provide the Services pursuant to the Enterprise Agreement; provided, however, that Business Associate shall not disclose PHI in any manner that would constitute a violation of HIPAA if so disclosed by Covered Entity. Business Associate may disclose PHI: (i) for the proper management and administration of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; (ii) to carry out the legal responsibilities of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; or (iii) as Required by Law. To the extent that Business Associate discloses PHI to a third party pursuant to Section 2(b)(i) or (ii) above under Reasonable Assurances, Business Associate must obtain in writing, prior to making any such disclosure: (x) reasonable assurance from the third party that such PHI will be held in a confidential manner; (y) reasonable assurance from the third party that such PHI will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to such third party; and (z) an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of such PHI, to the extent the third party has obtained knowledge of such breach (collectively, "Reasonable Assurances"). Except as Required by Law, Business Associate shall not disclose PHI to a health plan for payment or healthcare operations if the individual subject to the PHI has requested such restriction, the individual (or designee) pays out of pocket in full for the health care item or service to which the PHI relates, and the restriction has been made known to Business Associate in accordance with Section 3(b) of this BA Agreement.

C. De-identification. Business Associate may de-identify PHI in accordance with 45 CFR § 164.514.

D. Appropriate Safeguards. Business Associate shall comply with the applicable provisions of the Security Rules and shall implement appropriate administrative, technical, physical, and security safeguards in compliance with HIPAA that reasonably and appropriately safeguard and protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. As required by HIPAA, Business Associate shall maintain policies, procedures and documentation that address these safeguards and the requirements of HIPAA and which are appropriate to the size and complexity of Business Associate's operations and the nature and scope of its services.

E. Business Associate's Agents and/or Subcontractors. To the extent Business Associate uses one or more subcontractors or agents to provide Services to Covered Entity, and such subcontractors or agents create, receive, maintain, or transmit PHI, Business Associate shall require in accordance with 45 CFR § 164.308(b) and 164.502(e) that each subcontractor or agent agree to be bound by substantially the same restrictions as imposed by the terms of this BA Agreement and HIPAA on Business Associate. Following the discovery of non-compliance by a subcontractor or agent of any of its obligations with respect to PHI, Business Associate shall report such non-compliance to Covered Entity.

F. Access to PHI. Within ten (10) days of receipt of a request, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, available to Covered Entity for inspection and/or copying to enable Covered Entity to fulfill its obligations under 45 CFR § 164.524. If a request for access to PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity. Business Associate shall provide access to a copy of electronic PHI maintained by Business Associate in a Designated Record Set to the Covered Entity in accordance with the provisions of this Section and HIPAA.

G. Amendment of PHI. Within ten (10) days of receipt of a request, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, available to Covered Entity for amendment to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. Business Associate shall amend PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, as directed by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. If a request for amendment of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity.

H. Accounting of PHI Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Within ten (10) days of receipt of a request by Covered Entity, Business Associate shall make available to Covered Entity the information required to provide an accounting of such disclosures. Any accounting information shall include the information described in 45 CFR § 164.528(b), including, without limitation: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the written request for disclosure. If a request for an accounting of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity.

I. Governmental Access to Records. Business Associate shall make PHI and its facilities, internal practices, books, records, accounts, and other information relating to the use and disclosure of PHI available to the Secretary in a time and manner designated by the Secretary and shall cooperate with the Secretary concerning any investigation designed to determine Covered Entity's or Business Associate's compliance with HIPAA.

J. Minimum Necessary Use and Disclosure Requirement. In accordance with 45 CFR § 164.502(b), Business Associate shall only request, use and disclose the minimum amount of PHI necessary to reasonably accomplish the purpose of the request, use or disclosure. Further, Business Associate will restrict access to PHI to those employees, contractors, or agents of Business Associate who are actively and directly participating in providing Services to Covered Entity and who need to know such PHI in order to fulfill such responsibilities.

K. Retention of PHI. Business Associate shall retain all PHI throughout the term of the Enterprise Agreement and shall continue to maintain the information required under Section 2(h) of this BA Agreement for a period of six (6) years from its creation.

L. Notification Obligations; Mitigation. During the term of this BA Agreement, Business Associate shall notify Covered Entity within five (5) days (or such shorter time period as required by applicable State law) after the discovery of any use and/or disclosure of PHI not permitted by this BA Agreement, a Breach of Unsecured PHI, or any material Security Incident and shall provide Covered Entity with information regarding the improper use and/or disclosure, Breach or Security Incident as required by law. Business Associate shall take corrective action to mitigate and cure, if possible, any harmful effect that is known to Business Associate of an improper use and/or disclosure of PHI, Breach, or Security Incident. Business Associate shall cooperate with Covered Entity regarding any Breach notification to third parties, and shall reimburse Covered Entity for any reasonable notification costs incurred by Covered Entity in complying with the applicable requirements of HIPAA resulting from a Breach of Unsecured PHI by Business Associate. Business Associate shall be deemed to discover a Breach of Unsecured PHI as of the first day on which such Breach is known, or should have been known, by Business Associate.

M. Additional Obligations. Business Associate shall comply with the requirements of HIPAA, which are applicable to Business Associate as a business associate of the Covered Entity, including all regulations which are issued to implement such requirements, as may be amended, modified or superseded from time to time. To the extent Business Associate carries out one or more of Covered Entity's obligation(s) under 45 CFR Part 164, Subpart E, in the performance of such obligations, Business Associate shall comply with the requirements of 45 CFR Part 164, Subpart E, that apply to Covered Entity to the same extent as required by Covered Entity. Business Associate shall comply will all State laws that affect the privacy or security of PHI received from the Covered Entity.

N. Compliance with Standard Transactions. If Business Associate conducts, in whole or in part, Standard Transactions (as such term is defined in the Standards for Electronic Transactions Rule at 45 CFR Parts 160 and 162, as may be amended, modified or superseded, from time to time) for or on behalf of Covered Entity, Business Associate will comply, and will require any of its subcontractors or agents involved with such Standard Transactions on behalf of Covered Entity to comply, with each applicable

requirement of 45 CFR Parts 160 and 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked "not used" in a Standard Transaction or are not in the Standard Transactions' implementation specification; or (iv) changes the meaning or intent of the Standard Transactions' implementation specifications.

III. Obligations of Covered Entity.

A. Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

B. Restrictions on Use or Disclosure. Covered Entity shall only disclose PHI to Business Associate or to others, pursuant to this BA Agreement, in a manner and to an extent permitted by HIPAA. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individuals to use and/or disclose PHI, to the extent such changes or revocations may affect Business Associate's permitted or required uses and/or disclosures of PHI. Further, Covered Entity shall notify Business Associate of any restriction to the use and/or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's permitted or required uses and/or disclosures of PHI.

IV. **Term and Termination.**

A. Term. This BA Agreement shall commence on the Effective Date and will remain effective for the entire term of the Enterprise Agreement, unless earlier terminated in accordance with the terms herein.

B. For Cause Termination Due to Material Breach. Either party may terminate this BA Agreement by notice in writing to the other party, if the other party materially breaches this BA Agreement in any manner and such material breach continues for a period of thirty (30) days after written notice is given to the breaching party by the other party specifying the nature of the breach and requesting that it be cured. If termination of this BA Agreement is not feasible, the non-breaching party shall report the breach to the Secretary if required by HIPAA.

C. Effect of Termination. Upon termination of this BA Agreement, Business Associate shall return or destroy all PHI (regardless of form or medium), including all copies thereof and any data compilations derived from PHI and allowing identification of any individual who is the subject of the PHI. The obligation to return or destroy all PHI shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. If the return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon notification that return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this BA Agreement to such information and limit further uses or disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for as long as Business Associate maintains such PHI. If Business Associate elects to destroy the PHI, Business Associate shall notify Covered Entity in writing that such PHI has been destroyed.

V. **Construction.** This BA Agreement shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this BA Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA.

VI. **Captions.** The captions contained in this BA Agreement are included only for convenience of reference and do not define, limit, explain or modify this BA Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this BA Agreement.

VII. **Notice.** All notices and other communications required or permitted pursuant to this BA Agreement shall be in writing, addressed to the party at the address set forth at the end of this BA Agreement, or to such other address as any party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be sent by: (i) registered or certified mail, return receipt requested, postage pre-paid; (ii) overnight mail by a reputable carrier; (iii) facsimile with a copy sent by First Class Mail, postage pre-paid; or (iv) hand delivery. All notices shall be effective as of the date of delivery if by hand delivery or overnight mail, two (2) days following the date of facsimile, or if by certified mail on the date of receipt, whichever is applicable.

VIII. **Assignment.** This BA Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred by either party without the prior written consent of the other party and any assignment or transfer without proper consent shall be null and void.

IX. **Governing Law.** This BA Agreement shall be governed by, and interpreted in accordance with HIPAA and the internal laws of the State in which the Business Associate has its principal office, without giving effect to any conflict of laws provisions.

X. **Binding Effect; Modification.** This BA Agreement shall be binding upon, and shall enure to the benefit of, the parties hereto and their respective permitted successors and assigns. This BA Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event any provision of this BA Agreement shall conflict with the requirements of HIPAA, this BA Agreement shall automatically be deemed amended as necessary to conform to such legal requirements at all times.

XI. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

XII. **Severability.** In the event that any provision or part of this BA Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this BA Agreement, with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

XIII. **No Third-Party Beneficiaries.** Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person or entity other than Covered Entity, Business Associate and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

XIV. Counterparts. This BA Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which together shall constitute but one BA Agreement.

Entire Agreement. This BA Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written agreements, negotiations, commitments, and understandings.

IN WITNESS WHEREOF, Covered Entity and Business Associate have each caused this BA Agreement to be executed in their respective names by their duly authorized representatives as of the Effective Date.

BUSINESS ASSOCIATE:
Tritan Software International, Ltd.
Signature: DocuSigned by: 57BCF98A8A16499...
Print Name/Title Andrew L. Carricarte

Address: PO Box 13197
South City DSU
Cork, IE T12 C825

Telephone: +1.305.699.5000 Ext: 8100
Facsimile: +1.305.890.1806
Contact Person: Cristina Wallis

COVERED ENTITY:

Signature: _____
Print Name/Title: _____
Address: _____

Telephone: _____
Facsimile: _____
Contact Person: _____

<<STANDARD CONTRACTUAL CLAUSES>>

1. DEFINITIONS

For the purposes of the Clauses:

(a) **personal data**, **special categories of data**, **process/processing**, **controller**, **processor**, **data subject** and **supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) **the data exporter** means the controller who transfers the personal data;

(c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **technical and organizational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in ***Annex A*** which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

The data subject can enforce against the data exporter this *Clause 3*, *Clause 4(b)* to *Clause 4(i)*, *Clause 5(a)* to *Clause 5(e)* and *Clause 5(g)* to *Clause 5(j)*, *Clause 6.1* and *Clause 6.2*, *Clause 7*, *Clause 8.2* and *Clause 9* to *Clause 12* as third-party beneficiary.

The data subject can enforce against the data importer this *Clause*, *Clause 5(a)* to Clause 5(e), and *Clause 5(g)*, *Clause 6*, *Clause 7*, *Clause 8.2* and *Clause 9* to *Clause 12*, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this *Clause 3.1*, *Clause 5(a)* to *Clause5(e)*, and *Clause 5(g)*, *Clause 6*, *Clause 7*, *Clause 8.2*, and *Clause 9* to *Clause 12*, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in ***Annex B*** to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to *Clause 5(b)* and *Clause 8.3* to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of *Annex B* and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with *Clause 11* by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with *Clause 4(a)* to *Clause 4(i)*.

5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in *Annex B* before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

- **(i)** any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- **(ii)** any accidental or unauthorized access; and
- **(iii)** any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of *Annex B* which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with *Clause 11*; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. LIABILITY

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in *Clause 3* or in *Clause 11* by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in *Clause 3* or in *Clause 11* because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in *Clause 3* or in *Clause 11* because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. MEDIATION AND JURISDICTION

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. COOPERATION WITH SUPERVISORY AUTHORITIES

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in *Clause 5(b)*.

9. GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely .....

10. VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11. SUB-PROCESSING

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in *Clause 3* for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of *Clause 6* against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to *Clause 5(j)*, which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and

the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

DATA IMPORTER:

Tritan Software International, Ltd.

Signature: DocuSigned by: 57BCF98A8A16490...

Print Name/Title Andrew L. Carricarte

Address: PO Box 13197
South City DSU
Cork, IE T12 C825

Telephone: +1.305.699.5000 Ext: 8100

Facsimile: +1.305.890.1806

Contact Person: Cristina Wallis

DATA EXPORTER:

Signature: _____

Print Name/Title: _____

Address: _____

Telephone: _____

Facsimile: _____

Contact Person: _____

ANNEX A
[TO THE STANDARD CONTRACTUAL CLAUSES]

This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this *Annex A*.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer)
……
……
……

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):
The data importer provides maritime software. In particular, the data importer provides software for individual and organizational health and safety management.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
Crew, passengers, contractors, agents and/or employees of maritime vessels operated by the data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):
First, middle and last name, Title, Position, Employer, Contact information (company, email, phone, physical business address), ID data, Professional life data, Personal life data, Localization data.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
Data exporter may submit special categories of data to the data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, religious or philosophical beliefs, or trade-union or insurance membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data regarding health, included but not limited to; diagnoses, medical history, diagnostic results, treatments, prescriptions, etc., or data concerning a natural person's sex life or sexual orientation.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
The objective of Processing of Personal Data by data importer is for the performance of the Solutions pursuant to the Agreement.

ANNEX B
[TO THE STANDARD CONTRACTUAL CLAUSES]
This *Annex B* forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with *Clause 4(d)* and *Clause 5(c)* (or documents/legislation attached):

1. Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control):

- The data importer has implemented robust security protocols for all data centers, offices and other buildings from which data of the data exporter may be accessed.
- The security protocols include physical protection of buildings against break-ins, as well as access control systems. Security perimeters are established around IT systems hosting personal data. Additionally, the data centers utilized by the data importer maintains an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week and certifications with SSAE16/ISAE 3402 Type II, SOC 2, SOC 3 public audit report, as well as ISO 27001. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly. This also includes formal access procedures for allowing physical access to the data center
- The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only data importer authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved. The electronic card key and biometric access control system is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity. The data importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The IT systems and networks used for the processing of personal data are protected by anti-virus software, anti-malware software, firewalls and intrusion-detection-systems. The data importer also performs an annual Application Vulnerability Assessment Audits via an accredited third party to ensure there are no application vulnerabilities available for exploit.
- The data importer has a Strong Password Policy with a minimum length and character use requirement that ensures that the passwords are non-obvious and complex creating a very difficult scenario that deters human and technical automation discovery. The data importer further requires a scheduled and routine change of passwords to further deter unauthorized access. Employees are also required to take extra measures to guard their credentials carefully and ensure that their accounts are never compromised. These measures include the prohibition of shared access, written passwords or their electronic exchange.
- Devices used to access to data importer's assets must be password protected, in compliance with data importer's Strong Password Policy. The device must lock itself with a password or PIN if it's idle for five minutes. After five failed login attempts, the device should lock

2. Measures to prevent data processing systems from being used without authorization (access control):

- Any access to protected information is restricted to the purposes of performing that individual employee or contractor's responsibilities and only with the prior consent of the data exporter. Activity within the data importer's assets are recorded through a series of audit logs and routinely reviewed for abnormal activity. For all protected information such as medical and personal records, the data importer's employees and contractors are prohibited from access to this information unless required for the purpose of performing their responsibilities in accordance with the parties' agreements.
- Critical access information such as passwords are stored in an encrypted format within secured databases in order to prevent unauthorized access which also includes the restriction of administrator access.

3. Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control):

- The data importer's employees and contractors are provided access to the data importer's assets or software instances solely on an individually required, pre-authorized and restricted basis. They are prohibited from sharing accounts or providing individual accounts to any user without the authorization and approval from the data protection officer (or equivalent). Additionally, the data importer implements a role-based user access management for systems with access rights on a strict need-to-know basis.
- All personal data is encrypted at rest using 256 bit AES encryption. - The data importer diligently monitors the activities of all employees, to include audit records, activity logs and extensive background checks both prior and during employment.

4. Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control):

- All personal data is encrypted during transmission using strong encryption protocols. The Software is required to operate under an SSL Security Certificate utilizing 128-bit encryption. This certificate is authenticated and verified by a publicly accredited certificate authority. The connection uses TLS 1.2 and is encrypted using with SHA for message authentication and RSA as the key exchange mechanism. Secure transmission protocols are used, implementing Perfect Forward Secrecy (PFS). Only SSL encrypted channels are permitted for authorized viewing or accessing of personal data via the Software.
- Only authorized secure channels are permitted by data importer's policies for the transmission of personal or protected data. Unsecure transmission channels such as email or FTP are not permitted for the transmission of data unless secondary means have been utilized to appropriately secure the data from unauthorized access. These measures must conform to the strong encryption requirements with appropriate minimum length encryption keys as stipulated by the data importer's policy. Remote access to any hosted data or data on shipboard instances will exclusively take place using secure VPN encryption (AES256).
- The data importer logs transmission activities and transmission rights and regularly reviews these to ensure full compliance.

5. Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control):

- A comprehensive user account control and audit capability is established by the data importer. The data importer monitors the activities of all employees and contractors, to include audit records and activity logs. The recorded logs allow the data importer to verify the activity, time/date and manner in which personal data has been input, modified or removed.

6. Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control):

- The data importer shall ensure that any personnel entrusted with processing the data exporters' data have undertaken to comply with the principle of data secrecy and have been duly instructed on the applicable data protection regulations and the sensibility of data relating to health. The undertaking to secrecy shall

continue after the termination of the data processing.

- The data importer shall maintain a data protection officer (or equivalent) and implement regular internal controls to ensure that adequate data security measures remain in place at all times and that the data of the data exporter is only processed according to the instructions of the data exporter.
- The data importer's access to data is restricted to the provision of services pertaining to the agreement between the parties for the support and maintenance of the Software.
- The data importer monitors the activities of all employees and contractors, utilizing measures such as audit records and activity logs.

7. Measures to ensure that personal data are protected from accidental destruction or loss (availability control):
   - Data importer will replicate data over multiple redundant systems to protect against system failure or accidental destruction or loss. Any data hosted by the data importer for the data exporter are to be securely and regularly backed-up. Backups are stored in locations different from the location of the live systems.
   - The data centers utilized by the data importer is protected against accidental destruction by fire and flooding and have a redundant climate control unit, a surge protection and an uninterrupted power supply. The infrastructure systems that have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The services are designed to allow the data center to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

8. Measures to ensure that data collected for different purposes can be processed separately:
   - The IT systems used to host and/or process the data of the data exporter are physically and logically separated from IT systems used to process data of other clients of the data importer. - Test environments are logically separated from live environments and have a separate set of access credentials with appropriate levels of security.

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.