

SaaS Terms and Conditions

1. Definitions.

The following terms shall have the following meanings as set forth below:

“**Affiliates**” means any entity that directly or indirectly controls, is controlled by, or is under common control with another legal entity.

“**Agreement**” means this SaaS Terms and Conditions, its Exhibit(s), and any attached Order Forms(s).

“**Client**” means the party named as “Client” on one or more attached Order Form(s).

“**Confidential Information**” means business information, technical information and/or ideas which are not known to the public, including but not limited to:

(a) The terms and conditions of this Agreement;

(b) Specifications, algorithms, Documentation, source and object code for any ISONAS product that exists or is in development;

(c) The trade secrets and other “know-how” of ISONAS;

(d) Client’s data, material, content and cost models; and

(e) Any other information deemed “Confidential” by the disclosing party and not revealed to the general public, which the receiving party obtained through this Agreement; except information the receiving party can document (i) is in the public domain through no fault of the receiving party; (ii) was properly known to the receiving party, without restriction, prior to disclosure by the disclosing party; (iii) was properly disclosed to the receiving party by another person without restriction; (iv) is disclosed under operation of law; or (v) is disclosed by the receiving party with the disclosing party’s prior written approval.

“**Documentation**” means collectively, the operation instructions, user manuals, help files and other technical information and materials, in written or electronic form, delivered with access to the Software and that are intended by ISONAS for use in connection with the Software.

“**ISONAS**” means ISONAS Inc., with an address at 4750 Walnut Street, Suite 110, Boulder, Colorado 80301.

“**Effective Date**” means the date set forth on an attached Order Form.

“**Expiration Date**” means the date set forth on an attached Order Form.

“**Order Form**” means one or more fully executed purchase order for the Services attached to these terms and conditions and incorporated herein.

“**Services**” means the services described herein and in Exhibit 1.

“**Software**” means the machine-readable version of any and all software and all corrections, alterations, translations, upgrades and updates and any Documentation now or hereafter developed by ISONAS.

2. Client Obligations.

2.1 Use of the Services. Client agrees to comply with the terms for the Services set forth in Exhibit 1 hereto.

2.2 Compliance with Laws. both parties shall comply, and ensure its end users comply, with all applicable laws and regulations.

2.3 Security. Client is responsible for all information and content processed by Client or its end users through the Services (collectively, “**Client Information**”). Client shall be at all times responsible for all use of and access to the Services by its end users. Client shall control and manage access to the Services and to all Client Information stored within, or accessible through, the Services, both in determining the implementation configuration of the Services and through Client’s selection and adoption of its end users’ credentials and password practices. Client acknowledges that Client’s and its end users’ data security may be compromised if Client elects an open configuration, or if Client’s end users do not follow all recommended, reasonable, or applicable security policies and procedures and take other appropriate steps to maintain the security of the Services and the Client Information, including, without limitation, maintaining the confidentiality of Client’s end user identifications and passwords, frequent changing of passwords, and maintaining appropriate internal controls to monitor access to and use of the Services. Client shall be fully responsible for the protection of all end user identification, credentials and passwords for the Services. Client shall immediately notify ISONAS of any unauthorized access to the Services or to its end user identification, credentials or passwords. Client shall at all times use its best efforts to prevent unauthorized access to and disclosure of and maintain the security of the Services. Client shall promptly notify ISONAS in writing of any unauthorized use of, or any claim or proceeding involving the Services of which Client is or becomes aware. Client shall cooperate and assist ISONAS with the termination of any such unauthorized use. ISONAS is responsible for access to the Services by its employees and its subcontractors. In the event of a breach of the Services for which ISONAS is responsible, ISONAS shall promptly notify Client in writing of such breach.

2.4 Security Incident Response Provisions

(a) Client Personal and Client Proprietary Information

(1) Definition. Client Personal and Client Proprietary Information is defined as any information in the possession or under the control of Client or any of its Affiliates, or that is furnished or made available by Client or any of its Affiliates to ISONAS, i) identifying, ii) relating to, iii) describing, or iv) is capable of being associated with, any particular individual (whether Client employee, customer, or otherwise) or Client, including, but not limited to, name, signature, social security number, address, telephone number, passport

number, driver's license or state identification card number, insurance policy number, medical information or health insurance information, education, employment, employment history, bank account number, any other financial information, or any project related information. Nondisclosure of Client Personal and Client Proprietary Information. Despite any other provision in the Agreement, ISONAS's nondisclosure obligations with respect to Confidential Information that is also Client Personal and Client Proprietary Information shall survive any expiration or termination of the Agreement in perpetuity. Upon the expiration or termination of the Agreement, or at any time upon request of Client, all Client Personal and Client Proprietary Information in any medium, including all copies or parts of the Client Personal and Client Proprietary Information, shall be returned to Client or destroyed except that ISONAS may retain one copy of any materials prepared by ISONAS containing or reflecting Client Personal and Client Proprietary Information if necessary for compliance with its internal record-keeping or quality assurance requirements only. If destroyed, the destruction shall be certified in writing by ISONAS and such certification shall be delivered to Client with ten (10) business day.

(b) Security Incidents

(1) Security Incident Response Plan: ISONAS shall develop, implement and maintain a written plan and process for preventing, detecting, identifying, reporting, tracking and remediating Security Incidents ("Security Incident Response Plan" or "SIRP"). A Security Incident shall mean an event or set of circumstances resulting in a reasonable expectation of a compromise of the security, confidentiality or integrity of Client Personal and Client Proprietary Information under ISONAS's control. Examples of Security Incidents include:

- (i) Security breaches to ISONAS's network perimeter or to internal applications resulting in potential compromise of Client data or information;
- (ii) Loss of physical devices or media, e.g., laptops, portable media, paper files, etc., containing Client data;
- (iii) Lapses in, or degradation of, ISONAS's security controls, methods, processes or procedures;
- (iv) The unauthorized disclosure of Client Personal and Client Proprietary Information; and
- (v) Any and all incidents adversely affecting Client's or its Affiliates', as the case may be, information assets.

(2) SIRP General Requirements: ISONAS's SIRP will include Security Incident handling and response procedures, specific contacts in an event of a Security Incident, the contacts' roles and responsibilities, and their plans to notify Client or its Affiliates, as the case may be, concerning the Security Incident. The SIRP must be based on and meet all requirements of the following:

(i) U.S. federal and applicable state laws, statutes and regulations concerning the custody, care and integrity of data and information. ISONAS shall ensure that its SIRP and its business practices in performing work on behalf of Client comply with California's Information Practices Act of 1977, California Civil Code §§ 1798.80 et seq., which addresses the provision of notice to Client or its Affiliates, as the case may be, of any breach of the security of Client Personal and Client Proprietary Information if it is reasonably believed to have been acquired by an unauthorized person.

(ii) Client information management and information security policies and procedures as made available to ISONAS upon ISONAS's request ("Client Policies and Procedures").

(3) ISONAS Response to Security Incident. The following will apply in the event of a Security Incident:

(i) ISONAS will submit a Security Incident Report (SIR) to Client's or its Affiliates', as the case may be, in accordance with Client Policies and Procedures and applicable laws. The SIR shall be given promptly upon discovery of an SI as required by applicable laws and keep Client or its Affiliates, as the case may be, informed of developments and new information.

(ii) At Client's or its Affiliates', as the case may be, request, ISONAS will meet with Client or its Affiliates to discuss the cause of the Security Incident, ISONAS's response, lessons learned and potential improvements to ISONAS's system security processes and procedures.

(4) Compromise of Client Personal and Client Proprietary Information.

(i) Additional SIRP Requirements for Client Personal Information. With respect to any Client Personal and Client Proprietary Information in the possession or under the control of ISONAS, to protect Client Personal and Client Proprietary Information from unauthorized access, destruction, use, modification or disclosure, ISONAS shall:

Develop, implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Client Personal and Client Proprietary Information from unauthorized access, destruction, use, modification, or disclosure;

Develop, implement and maintain data privacy and security programs with administrative, technical, and physical safeguards appropriate to the size and complexity of the ISONAS's business and the nature and scope of ISONAS's activities to protect Client Personal Information from unauthorized access, destruction, use, modification, or disclosure;

(ii) Notice Requirements for Client Personal and Client Proprietary Information. In the event of a Security Incident where Client Personal and Client Proprietary Information was, or is reasonably believed to have been, acquired by an unauthorized person, ISONAS shall immediately provide the SIR required by Section 2 (C) of this Exhibit. This SIR shall state Client Personal and Client Proprietary Information may be involved, and shall describe the suspected nature of the Client Personal and Client Proprietary Information.

(5) SIRP Review. At Client's or its Affiliates', as the case may be, request, ISONAS shall review the SIRP at least annually with designated representatives to identify updates, changes or potential improvements; and a process to document these changes within ninety (90) days of these changes.

(6) Document Retention. ISONAS shall maintain all documentation relating to Security Incidents, whether in written or electronic form, including their identification, processing and resolution, for two (2) years after final resolution of all Security Incidents, including the final resolution of all claims arising out of any Security Incident.

(c) Compliance. ISONAS shall ensure that its employees, agents and contractors performing services for ISONAS in connection with the Order Form are informed of and comply with these Security Incident provisions.

3. ISONAS Obligations.

3.1 Services. ISONAS will provide the Services as described in Exhibit 1.

3.2 Suspension and Termination. ISONAS reserves the right to suspend or terminate access to and use of the Services if ISONAS believes that Client or any of its end users have undertaken, or participated in, any of the activities prohibited in this Agreement, violated the terms of this Agreement, or whose actions have, or are likely to, otherwise cause any harm to or claim against ISONAS, the Services, or any third party. ISONAS reserves the right (but does not undertake an obligation) at its sole discretion to monitor the activities of Client's end users of the Services, and the Client Information processed by Client using the Services.

3.3 Copy of Client Data. At any time during the term of this Agreement, Client may request a copy of the Client data provided pursuant to the Services. Within two (2) business days of such request, ISONAS will provide Client a copy of such Client data.

4. Fees and Payments

4.1 Fees. Fees for the Services are as specified in the applicable Order Form, and apply for the duration specified in the Order Form.

4.2 Payments. All fees for the Services will be due and payable by Client to ISONAS (i) within thirty (30) days of Client's receipt of invoice, (ii) in the currency specified in an Order Form, and (iii) by wire transfer of funds to an account designated by ISONAS or by check sent to an address designated by ISONAS. Invoices may be delivered by email or other electronic means. Client is responsible for all sales, use or similar taxes imposed by any governmental entity on the transactions contemplated by this Agreement, excluding taxes based on ISONAS' net income, revenues or employee base. If Client fails to pay an invoice within sixty (60) days after the date of the invoice, ISONAS reserves the right, after providing seven (7) days' written notice to Client, to suspend Client's access to or use of the Services.

5. Proprietary Rights; Confidentiality; Trademarks.

5.1 Ownership. As between ISONAS and Client, ISONAS has, and shall retain, all right, title and interest in and to the Services, any trade secrets, inventions or know-how (whether patentable or not) or Software incorporated or used in the Services, and all intellectual property and other proprietary rights (including, without limitation, trademarks, trade names, moral rights, copyrights and patent rights) in any of the foregoing arising under the laws of the United States or anywhere throughout the world.

5.2 Confidentiality. Each party agrees that, except upon the prior express written approval of the other party, the receiving party will hold in the strictest confidence, and shall not disclose to any person, firm, corporation or other entity, any Confidential Information received in connection with this Agreement. Client further agrees that Client will not reverse engineer or attempt to derive the composition or underlying information, structure or ideas of the Services. Disclosure of Confidential Information by the disclosing party to the receiving party does not grant the receiving party a license in or to any of the Confidential Information. If, in the course of this Agreement, it is ever unclear to the receiving party whether certain information is Confidential Information, the receiving party will ask a principal of the disclosing party whether the information is Confidential Information and the receiving party will treat such information as Confidential Information unless and until the receiving party is told in writing that such information is not Confidential Information.

5.3 Nondisclosure. The receiving party agrees that the receiving party shall:

(a) use Confidential Information only in the manner and for the purposes specified in the disclosure made to the receiving party;

(b) advise each employee or other person with access to Confidential Information of the obligation to protect it;

(c) use, and require others to use, due care to protect all Confidential Information; and

(d) promptly notify the disclosing party of any unauthorized release of Confidential Information.

5.4 Duties Upon Termination of this Agreement. Upon termination of this Agreement, the receiving party agrees that the receiving party will exercise reasonable care to return to the disclosing party all documents or articles containing Confidential Information, or destroy such documents or articles containing Confidential Information and certify to the disclosing party that it has done so.

5.5 Enforcement. The parties further agree that:

(a) the restrictions set forth in this Agreement protect the legitimate interests of the disclosing party and impose no undue hardship on the receiving party;

(b) the restrictions set forth in this Agreement are reasonable as to scope and duration; and

(c) due to the unique nature of Confidential Information, any breach of this Agreement would cause irreparable harm for which damages are not an adequate remedy and that the disclosing party shall therefore be entitled to an injunction or other equitable relief in addition to all other remedies available at law.

5.6 Restrictions. ISONAS has represented to Client that it has expended great expense in creating the Software and the Services and has a proprietary interest therein. Client acknowledges that the Software is copyrighted and contains trade secrets of ISONAS. Client covenants that it will not sublicense, disclose, display, copy, distribute or use the Software or the Services for any other purpose than that described herein and will hold in strict confidence the design, specifications and associated Documentation of the Software and Services. Neither Client, nor any third party, shall modify, adapt, translate, prepare derivative works from, decompile, reverse engineer, or otherwise attempt to derive the source code from the Software. Neither Client, nor any third party, shall remove, obscure or alter ISONAS' copyright notices, trademarks, trade names or other proprietary rights or notices affixed to or contained in the Software and/or the Services. Client shall not and shall not authorize any third party to: (i) create derivative works, as defined under 17 USC § 106 (as interpreted by applicable case law), copy (other than as set forth in this Agreement), alter or in any way modify the Software; (ii) translate, decompile, disassemble, reverse compile or reverse engineer the Software or the Services, or in any other manner reduce the Software or the Services to human perceivable form, except to the extent that such restrictions are not permitted under applicable law; or (iii) bypass or delete any copy protection methods that are for preventing unauthorized copying or use of the Software or the Services. Client further acknowledges and agrees that in the event of a breach or threatened breach by the Client of any of the provisions of this paragraph, ISONAS will have no adequate remedy at law and accordingly shall be entitled to injunctive relief. However, no specification in this Agreement of a specific legal or equitable remedy shall be construed as a waiver or prohibition against any other legal or equitable remedies in the event of the breach of any provision of this Agreement. The covenants contained in this paragraph shall survive the termination of this Agreement. Client shall take appropriate action whether by instruction, agreement or otherwise and whether with its employees or others, to satisfy its obligations under this Agreement with respect to the use, copying, protection and security of the Software, Services, Documentation and all materials related thereto.

Further, Client shall not, and shall not allow any others to: (a) interfere with or disrupt the integrity or performance of the Services; or (b) attempt to gain unauthorized access to the Services or its related systems or networks.

5.7 Reservation of Rights. Any and all rights in and to the Software, Documentation, and Services not expressly granted to Client in this Agreement are hereby reserved by ISONAS.

5.8 General Data Protection Regulation (GDPR). The end user is responsible for entering personal information into the ISONAS Pure Access Cloud portal. This data can include name, credential, phone number and / or email. Please see your company security administrator responsible for entering data into the ISONAS Pure Access Cloud system for exact details regarding custom fields that the security administrator may have created. The data is stored securely in the ISONAS Cloud platform and only stored for the explicit purpose of use within the ISONAS Pure Access Cloud application. No data is shared, processed or exposed. Data is retained in backups for 12 months at which time it is purged from the system. Data access is restricted to administrators that require access to maintain the system. ISONAS is not responsible for the on premise version (Pure Access Manager) as it is provided with no data and installed or configured on the customer's premises. Pure Access Manager is under the customers exclusive control. By inputting data into the ISONAS system the customer agrees that upon separation or deletion of data, the data will: (1) Delete from the primary system immediately, (2) Remain in near line backups for up to but not to exceed 48 hours where it is only accessible by ISONAS administrators, and (3) Remain in off line backups for up to but not to exceed 12 months where it is only accessible by ISONAS administrators.

6. Indemnification.

6.1 Indemnification by ISONAS. ISONAS shall indemnify, defend and hold harmless Client from and against all losses, liabilities, damages and claims, and all related costs and expenses (including any costs or expenses related to increased regulatory or administrative oversight), fines, penalties, or interest, including reasonable legal fees and costs, arising out of, in connection with, or relating to any claim involving performance or non-performance of the Services:

- (a) If the Services or any portion of the Services infringe upon or violate any trade secret, trademark, trade name, copyright, patent, or other intellectual property rights of any third party; or
- (b) Relating to any actual or alleged violation of any applicable law; or
- (c) Relating to visa status, payment or non-payment of any statutory withholding charges, Client employee benefits or other financial obligations, including overtime, contribution taxes, benefits and penalties payable under Workers' Compensation (including

Workers' Compensation Reform Act of 1989), unemployment compensation, disability benefit, old age benefit, or tax withholding laws if Client can be adjudged liable as an employer with respect to ISONAS or ISONAS personnel, arising out of or in any way related to the relationship between Client, ISONAS, and ISONAS personnel, including the failure of ISONAS personnel to be recognized as exclusively employed by ISONAS and not by Client.

6.2 Infringement. If the Services, or any portion of the Services becomes, or in Client's reasonable opinion is likely to become, the subject of an infringement, including misappropriation, claim or proceeding, ISONAS shall, in addition to indemnifying Client as provided in this section and any other rights Client may have under the Agreement: (i) promptly at ISONAS' expense secure the right to continue using the Services; or (ii) if this cannot be accomplished with commercially reasonable efforts, then, at ISONAS' expense, replace or modify the Services to make the Services non-infringing, provided the replacement or modification will not degrade the performance or quality of the Services for any affected component of the Services; or (iii) if neither (i) or (ii) can be accomplished by ISONAS with commercially reasonable efforts, then, at Client's election, refund to Client the amount Client paid for the remaining term of the Services. The remedies provided in this section shall not limit ISONAS' indemnification obligations defined above.

6.3 Indemnification Procedures. The party seeking indemnification hereunder (the "**Indemnitee**") shall provide the other party (the "**Indemnitor**") with: (i) prompt written notice of any claim subject to indemnification; provided, however, the Indemnitor shall not be required to indemnify Indemnitee to the extent any delay in providing such notification increases the amount of any such claim; and (ii) reasonable assistance to defend or settle such claim at the Indemnitor's expense. The Indemnitee agrees that the Indemnitor shall have sole control of the defense and all related settlement negotiations of such claim; provided, however, that the Indemnitor shall not agree to any settlement or compromise that imposes any obligation or liability on the Indemnitee (other than the payment of money that is indemnified or that impacts the use of the Software or the Services) without the Indemnitee's prior written consent, which shall not be unreasonably withheld. The Indemnitee shall have the right to participate in the defense and settlement negotiations of such claim through its own counsel at its own expense.

7. Term; Termination.

7.1 Term. This Agreement becomes effective on the Effective Date and expires on the
Expiration Date. This Agreement shall remain in effect for the Term set forth on the Order Form.

7.2 Termination for Convenience. Either party may terminate this Agreement, without
cause, by written notice to the other party at least thirty (30) days prior to the expiration of the then current Term, which termination will become effective at the end of the then current Term.

7.3 Termination for Material Breach. In the event of any material breach of this Agreement (including any Order Form), the non-breaching party shall give the breaching party written notice describing such breach. In the event that the breaching party fails to cure such breach within fifteen (15) days after receipt of written notice of such breach from the non-breaching party, the non-breaching party may terminate this Agreement upon written notice to the breaching party.

7.4 Effect of Termination. Upon the effective date of any termination or expiration of this Agreement, without prejudice to any other rights which the parties may have, and subject to the other provisions of this Agreement: (i) ISONAS shall immediately discontinue providing Services to Client; (ii) Client shall immediately discontinue any and all use of the Services, and return any Documentation to ISONAS; and (iii) Client shall pay ISONAS any outstanding amounts due hereunder. Further, within thirty (30) days of the effective date of any termination or expiration of this Agreement, ISONAS shall remove all Client data from the Services, and certify to Client in writing that it has done so.

8. LIMITATIONS OF LIABILITY.

8.1 WAIVER OF CONSEQUENTIAL DAMAGES. WITH THE EXCEPTION OF ISONAS' LIABILITY OBLIGATIONS REGARDING INFRINGEMENT INDEMNIFICATION AND RELATING TO THE ACTUAL OR ALLEGED VIOLATION OF ANY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, OR SPECIAL DAMAGES, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8.2 LIMITATIONS OF LIABILITY. WITH THE EXCEPTION OF ISONAS' LIABILITY OBLIGATIONS REGARDING INFRINGEMENT INDEMNIFICATION AND RELATING TO THE ACTUAL OR ALLEGED VIOLATION OF ANY APPLICABLE LAW, ISONAS' SOLE LIABILITY TO CLIENT, IF ANY, SHALL IN NO EVENT EXCEED THE AMOUNTS PAID HEREUNDER FOR THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT(S) GIVING RISE TO SUCH LIABILITY.

8.3 DISCLAIMERS. EXCEPT AS EXPRESSLY STATED HEREIN, ISONAS MAKES NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. ISONAS DOES NOT WARRANT THAT THE SERVICES WILL MEET ALL OF CLIENT'S REQUIREMENTS OR THAT THE USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.

9. Miscellaneous.

9.2 Entire Agreement. This Agreement shall be binding upon ISONAS and its successors and assigns, and Client, its successors and assigns, as the case may be. This Agreement, including any Order Forms or exhibits, represents the entire Agreement between the parties, and expressly supersedes and cancels any prior oral or written agreements on the subjects herein. Each party acknowledges that it is not entering into this Agreement on the basis of any representations not expressly contained herein. Other than as specified herein, this Agreement may only be supplemented or modified by a writing executed by the parties. No additional or conflicting term in any purchase order, or other document shall have any effect.

9.3 Governing Law, Venue. This Agreement shall be governed in accordance with the laws of the State of Delaware, without regard to its conflicts of law rules. The exclusive forum for any disputes, suits, actions or after legal proceeding arising out of or relating to this Agreement shall be an appropriate state or federal court situated in Denver County in the State of Colorado and each party hereby irrevocably submits to the exclusive jurisdiction and venue of any such court in any such dispute, suit, action or other legal proceeding.

9.4 Severability. If any provision of this Agreement or portion thereof is found to be invalid or unenforceable under applicable law, it shall be omitted from this Agreement without invalidating the remainder of such provision or the remaining provisions of this Agreement.

9.5 Headings. The various headings in this Agreement and any exhibits are for convenience only. They shall not affect the meaning or interpretation of this Agreement or any paragraph or provision hereof.

9.6 Counterparts/Execution. This Agreement may be executed in two (2) or more counterparts, each of which when so executed and delivered, including delivery of an executed counterpart by means of facsimile transmission or email delivery of an electronically scanned counterpart, shall be deemed an original, and all of which, together, shall constitute one and the same instrument. Upon mutual agreement of the parties, this Agreement may be executed and signed via electronic signature.

9.7 Force Majeure. Neither party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including acts of war, acts of God, earthquake, flood, embargo, riot, sabotage, governmental act or failure of the internet not resulting from the actions or omissions of the party.

9.9 Survival. Sections 1, 4, 5, 7.4, 8, this Section 9, and Section 10 of this Attachment 1 shall survive any termination of this Agreement.

9.10 Relationship. The parties intend to create an independent contractor relationship and nothing contained in this Agreement will be construed to make either ISONAS or Client partners, joint ventures, principals, agents or employees of the other. Neither party will have any right, power or authority, express or implied, to bind, or make representations on behalf of the other.

9.11 Export Laws. Client agrees to comply with all laws and regulations of the United States, European Union, and other countries and jurisdictions (“**Export Laws**”) to assure that the Services or the Software are not exported, directly or indirectly, in violation of Export Laws, or used for any purpose prohibited by Export Laws. ISONAS shall provide all information under its control and necessary or useful for Client to obtain any import or export licenses required for Client to export Services within ten (10) business days of Client’s request. In no event may Client sell or export, directly or indirectly, the Services or the Software to any of the following countries: Burma (Myanmar), Cuba, Iran, Sudan, Syria, Western Balkans, Belarus, Cote d’Ivoire, Democratic Republic of the Congo, Iraq, Liberia (Former Regime of Charles Taylor), Libya, North Korea, Somalia and Zimbabwe.

9.12 U.S. Government Restricted Rights. If the Services are used for or on behalf of the United States of America, its agencies and/or instrumentalities (“**U.S. Government**”), it is provided with RESTRICTED RIGHTS. The Services and accompanying documentation are “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to 48 C.F.R. 12.212 and 227.7202, and “restricted computer software” pursuant to 48 C.F.R. 52.227-19(a), as applicable. Use, modification, reproduction, release, performance, display, or disclosure of the Services and accompanying documentation by the U.S. Government are subject to restrictions as set forth in this Agreement and pursuant to 48 C.F.R. 12.212, 52.227-14 (Alternate III), 52.227-19, 227.7202, and 1852.227-86, as applicable.

9.13 Non-solicitation. During the term of this Agreement and for twelve (12) months after its expiration or termination, neither party will, either directly solicit for employment by itself any employee of the other party who was involved in the performance of the party’s obligations under this Agreement, unless the hiring party obtains the written consent of the other party. In the event that either party hires an employee of the other party, the hiring party shall pay the other party an amount equal to thirty percent (30%) of such employee’s first year’s salary. This provision shall not restrict general advertisements of employment or the rights of any employee of one party, on that employee’s own initiative, or in response to general advertisements, to seek employment from the other party and under such circumstances, for the other party to hire such employee.

9.14 Representation of Authority. Each party represents and warrants that: (i) the signatory named in an Order Form has the authority to bind the party on whose behalf he/she is signing to the terms of this Agreement; (ii) the execution and delivery of this Agreement has been duly authorized; and (iii) this Agreement is valid binding on the parties and enforceable in accordance with its terms.

10. Notices.

All notices delivered under this Agreement shall be in writing and deemed given upon receipt when delivered personally or upon confirmation of receipt following delivery of (i) nationally recognized overnight courier service, or (ii) registered or certified mail, return receipt

requested, postage prepaid, in each case addressed to the party's address set forth in an Order Form, or at such other address of which one party is notified by the other in writing.

Exhibit 1
Services

A. Software Functionality.

“Named Users”. Subject to the terms and conditions of this Agreement and upon payment in full of the fees set forth in one or more Order Form(s), Client may use the Services solely for Client’s business purposes for the number of Named Users as set forth in an Order Form and in the Documentation. As used herein, “Named User” means the end-user identified by name and authorized by Client to use the Services pursuant to the terms of this Agreement. Named Users may be de-activated by Client removing security profiles from end-user accounts. Once a Named User is de-activated, it can be re-activated by Client by allocating the license related to such de-activated Named User to any Named User account.

The online access rights to the Software located on ISONAS’ servers and the online services and functions offered in connection with the Software are further described in the Documentation. Such access rights may be subject to terms and conditions of third party services incorporated into the Services. Client agrees to comply with, and to ensure that its Named Users comply with, any such third party terms and conditions.

B. Additional Use Restrictions

The responsibility for avoiding harmful activities rests primarily with the Client. ISONAS will not, as an ordinary practice, monitor the communications of its subscribers to ensure that they comply with ISONAS policy or applicable law. When ISONAS becomes aware of harmful activities, however, it may take any action to stop the harmful activity, including but not limited to, removing information, shutting down a web site, implementing screening software designed to block offending transmissions, denying access to the internet, or take any other action it deems appropriate.

Material and Product Requirements. Client must ensure that all material and data placed on ISONAS' equipment is in a condition that is 'server-ready,' which is in a form requiring no additional manipulation by ISONAS. ISONAS will make no effort to validate any of this information for content, correctness or usability. If Client material is not 'server-ready,' ISONAS has the option at any time to reject this material. ISONAS will notify Client of its refusal of the material and afford Client the opportunity to amend or modify the material to satisfy the needs and/or requirements of ISONAS. Use of the Services requires a certain level of knowledge in the use of the Software. It is not ISONAS' responsibility to provide this knowledge or Client support outside of the Services.

Actions. ISONAS reserves the right and has absolute discretion to restrict or remove from its servers any content that violates this Agreement or related policies or guidelines, or is otherwise objectionable or potentially infringing on any third party's rights or potentially in violation of any laws. If ISONAS becomes aware of any possible violation by Client of this Agreement, any related

policies or guidelines, third party rights or laws, ISONAS may immediately take corrective action, including, but not limited to, (a) issuing warnings, (b) suspending or terminating the Service, (c) restricting or prohibiting any and all uses of content hosted on ISONAS' systems, and/or (d) disabling or removing any hypertext links to third-party web sites, any of Client content distributed or made available for distribution via the Services, or other content not supplied by ISONAS which, in ISONAS' sole discretion, may violate or infringe any law or third-party rights or which otherwise exposes or potentially exposes ISONAS to civil or criminal liability or public ridicule. It is ISONAS' policy to terminate repeat infringers. ISONAS' right to take corrective action, however, does not obligate ISONAS to monitor or exert editorial control over the information made available for distribution via the Services. If ISONAS takes corrective action due to such possible violation, ISONAS shall not be obligated to refund to Client any fees paid in advance of such corrective action.

Disclosure Rights. To comply with applicable laws and lawful governmental requests, to protect ISONAS' systems and Clients, or to ensure the integrity and operation of ISONAS' business and systems, ISONAS may access and disclose any information it considers necessary or appropriate, including, without limitation, user profile information (i.e., name, e-mail address, etc.), IP addressing and traffic information, usage history, and content residing on ISONAS' servers and systems. ISONAS also reserves the right to report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. If ISONAS, or any of its Affiliates are requested or required by applicable law, regulation, legal process, subpoena, or other directive of a court, administrative agency, quasi-judicial body, or arbitration panel to disclose the Client's Confidential Information, ISONAS, or its Affiliates will notify the Client promptly so that the Client may seek an appropriate protective order, or waive, in such instance, compliance by ISONAS or its Affiliate with the applicable provisions of this Agreement. In the event no protective order or other remedy is obtained, ISONAS or its Affiliates, under the advice of legal counsel, will furnish only that portion of the Clients Confidential Information that ISONAS is legally required to disclose. In any event, ISONAS or its Affiliates will cooperate with, and not oppose action by, the Client to obtain an appropriate protective order or other reliable assurance that confidential treatment consistent with this Agreement will be accorded the Confidential Information.

Interruption of Service. Client understands and agrees that occasional temporary interruptions of any internet services may occur as normal events in the provision of Internet services. Client hereby acknowledge and agree that under no circumstances will ISONAS be held liable to Client or any other person, firm or entity for any financial or other damages due to any temporary delay, outages or interruptions of the Services. Further, ISONAS shall not be liable to Client or any other person, firm or entity for any delay or failure to perform its obligations under this Agreement, where such delay or failure results from any cause or causes including, but not limited to, any act of God, fire, explosion, vandalism, cable cut, storm, or other cause beyond its reasonable control (including, without limitation, any mechanical, electronic, communications or third-party supplier failure); any law, order, regulation, direction, action or request of the United

States government or of any other government (including state and local governmental agency, department, commission, court, bureau, corporation or other instrumentality of any one or more of said governments) or of any civil or military authority; national emergencies, insurrections, riots, wars; or strikes, lockouts, or work stoppages or other labor difficulties; ISONAS failures, shortages, breaches or delays.

C. Software Support Services

In addition to the terms set forth in the body of the SaaS Terms and Conditions, the following terms shall apply with respect to Software support services:

1. Definitions

Updates means any upgrade, bug fix, error corrections, or modification to the Software that is generally made available to customers of ISONAS in the ordinary course of its business free of charge.

Upgrades means any upgrades or modifications to the Software which include feature enhancements or new functionality that are generally made available to customers of ISONAS in the ordinary course of its business for a fee.

Hours of Operation - Monday through Friday, 9:00AM through 8:00PM United States Eastern Time (ET), excluding national holidays observed by ISONAS. ISONAS may make reasonable changes to Hours of Operation from time to time. ISONAS shall provide no less than ten (10) business days' notice for any such changes.

SA (Support Analyst)- ISONAS Customer Support ("Customer Support") becomes fully engaged on the Effective Date set forth in the applicable Order Form, and is the main point of coordination for all support requests from Client. An SA is normally the first point of contact in the event that a Client needs assistance with the supported Software. The primary function of the SA is to perform a first level Problem determination, severity level determination, Problem resolution and then interface with any additional resources required, working towards the resolution of the Problem. In addition the SA can be called during Hours of Operation to give a status update on any ongoing Problems and is responsible for pro-actively obtaining any status updates.

Incident - An Incident is defined as a single-defined Problem seeking resolution.

Problem - A Problem is a failure of the Software to conform with ISONAS' published specifications for the Software in any material respect, or a failure of the Hosting Services to meet the terms in this Agreement.

Problem Report - Notification of a Problem that includes the following information: (1) a description of the Problem and the desired functionality the Client wishes to achieve, (2) the step-by-step process to reproduce the Problem, and (3) any and all exact error messages associated with the Problem.

Resolution - A Resolution to a Problem may consist of any of the following:

- Solution or answer is provided
- A request for enhancement is submitted
- A fix or work-around is provided
- An identified error in the Documentation is fixed
- A fix is incorporated into a future release (for Severity Three and Four only)
- The Problem relates to a third-party software vendor who has been notified of the problem

An Incident is considered "open" when a Client provides an SA with a Problem Report. An Incident is considered "closed" when a Resolution to the Problem is given to the Client. An Incident is also considered "closed" if and when it is determined that (a) the Problem Report relates to third party software that is not the Software or the Hosting Services, (b) the problem identified is not a Problem as defined herein, or is not covered by the Services or (c) the problem relates to a hardware/software issue that is not supported by ISONAS.

2. Client Services

ISONAS shall provide Client, so long as Client is in compliance with the terms of this Agreement, with the following services:

- a. Phone/Email/Web-based Support – Client shall have the opportunity to access a web-based portal, call or e-mail ISONAS to have questions answered about the operation of the Software. ISONAS will use commercially reasonable efforts to provide answers to Client's questions during Hours of Operation.
- b. Updates and Upgrades – Client shall be provided with any Updates (and Upgrades if Client has paid ISONAS for Services as set forth herein) that ISONAS makes generally available to its other customers and will install the Update or Upgrade in Client environments.
- c. Additional services – Client shall have the opportunity to contract with ISONAS to obtain additional professional services, including, implementation services, configuration, project management, and training at ISONAS' then prevailing rates. Such services are excluded from the Services.

Should Client alter the Software in any manner, ISONAS' obligation to provide the services described herein shall immediately cease.

3. Support Process

ISONAS requires that Client purchase an annual or one-time support contract. ISONAS will request that Client designate up to three (3) Client support representatives (“Client Designated Representatives”) who will be authorized to contact ISONAS’ Customer Support for support requests. The SA is the main point of coordination for all support requests and is the first point of contact in the event that a Client Designated Representative needs assistance with the Software or Hosting Services.

Client shall establish and maintain the organization and processes to provide “First Line Support” for the Software directly to end users. First Line Support shall include but not be limited to (a) a direct response to end users with respect to inquiries concerning the functionality or operation of the Software, (b) a direct response to end users with respect to problems with the Software, (c) a diagnosis of problems or deficiencies of the Software and (d) a resolution of problems or deficiencies of the Software.

ISONAS shall establish and maintain the organization and processes to provide “Second Line Support” for the Software to Client. If after commercially reasonable efforts Client is unable to diagnose or resolve problems or deficiencies of the Software, Client shall contact ISONAS’ SA (or other ISONAS support representative if SA is not available) for Second Line Support and ISONAS shall provide support for the Software in accordance with the terms herein.

Second Line Support shall be provided to up to three (3) Client Designated Representatives . ISONAS shall provide Second Line Support directly only to these Client Designated

Representatives. Second Line Support shall include but not be limited to (i) a diagnosis of Problems and (ii) a resolution of Problems.

4. ISONAS Customer Support Procedures

In order for Client to receive the highest level of responsiveness when contacting Customer Support, the following procedures are recommended:

- For telephone support during Hours of Operation, call the applicable ISONAS Support Line as designated on ISONAS’ website. If an SA is not immediately available, Client will have the option to open a support ticket and/or leave a message.
- For email support, send a question or issue to support@isonas.com. Such request will be logged and assigned to an SA.

5. Support Severity Levels

Severity One - A Problem exists that renders the Software inoperable or inaccessible. The Software is experiencing a total system failure as a result of a Problem and there is no work-around or reasonable alternative method available, or a key function or process immediately critical to the Client's business is not working as documented as a result of the Problem, causing the Client's business operations to be catastrophically impacted, and there are no workarounds or reasonable alternative method available.

Severity Two - A function is not working as documented as a result of a Problem, however, there is a work-around or reasonable alternative method available; or a function is not working as documented, and there is no work-around or reasonable alternative method available, however the use of the function is not immediately critical to the business, but the function is necessary.

Severity Three - A function is not working as documented as a result of a Problem, however, the Incident has a minor impact to the Client's business, but is requested to be fixed.

Severity Four - Client has a non-critical question, or a problem concerning the Software that has no impact to the Client's business.

6. Service Level Resolution Goals and Notification Procedures

The following Service Level Resolution Goals are designed to help ISONAS' support team drive cases to a timely Resolution. ISONAS exercises commercially reasonable efforts to meet the following response times but does not guarantee that the following response and resolution times will always be met.

Severity Level	Initial Response	Resolution Goal (if programming is not needed)	Resolution Goal (if programming is needed)
One	1 hour	24 hours	2 business days
Two	4 hours	2-3 business days	20 business days
Three	8 hours	6-8 business days	60 business days
Four	24 hours	8-12 business days	Future Release

(All of the response times are measured from the receipt of the support request.)

Severity Level One and Two Problems

Availability

SAs are available to be the first point of contact for Severity One and Two Problems. If the above stated goals are not met, the SA shall escalate to ISONAS Support Management who would be responsible for notifying the appropriate development leadership team members to alert them of the urgency of the problem and engage them accordingly.

Notification

Promptly following the receipt of a service call for a Severity One or Two Problem, the following people shall be notified:

ISONAS Support Manager

ISONAS Account Manager responsible for the

Client Severity Level Three and Four Problems

Availability

SAs are available during Hours of Operation to be the first point of contact for Severity Three and Four Problems.

7. Enhancement Requests

In addition to those Problems designated as Severity One through Severity Four, Client may designate Incidents as Enhancement Requests. Enhancement Requests are requests

to enhance or modify features of the supported Software including features that Client would like ISONAS to incorporate into future versions of the Software.

Enhancement Requests are to be submitted via e-mail to the SA assigned to Client. Upon receipt of an Enhancement Request, the SA will classify the request and submit it to the appropriate ISONAS personnel for response. Status on Enhancement Requests that have been submitted are available through the SA. ISONAS is not obligated to implement Enhancement Requests.

D. Hosting Services Description and Terms

Subject to this Agreement and the parameters and restrictions set forth in the Order Form, including without limitation, payment of the applicable fees for the Services, and in the Hosting Services Description and Terms set forth in this Section D, for the duration specified in the Order Form, ISONAS shall host the Software (the “**Hosting Services**”) and provide such Hosting Services as more fully described below. ISONAS shall not be responsible for any delay in, or inability to perform, any Hosting Services that results from a delay or failure in performance by Client, including any failure of Client to make management and technical personnel reasonably available to ISONAS.

1. Data Center Requirements

The Software will be hosted in a data center that meets the following requirements:

- (a) operated by prudent and experienced data center operators;
- (b) uninterruptible power (including UPS and generator power to maintain continuous power supplies during power outages or problems);
- (c) early warning smoke detection and shutdown systems;
- (d) computer accommodation with N+1 HVAC capabilities (heating, ventilation, air-conditioning and cooling);
- (e) security (physical, and network) security which includes high security access and video surveillance monitoring of the data center; and
- (f) fully redundant pathways to the internet.
- (g) fully configured firewalls to block non-essential traffic to secure access to the Software and provision of the Hosting Services.

2. Environments

- (a) ISONAS will provide Hosting Services for the number of Production Environments as set forth in an Order Form.
- (b) Uptime availability requirements as defined below will only apply to Production Environments.

3. Administration (network, systems, and database)

- (a) ISONAS will administer the operating systems to ensure they have security patches applied as soon as practicable taking into account potential

interference of implementing the patches to Client's use of the Software and the criticality of the relevant security issue that the patches are applied to address.

- (b) ISONAS will perform maintenance on the environments including but not limited to operating systems and databases that will adversely affect performance or availability during these "Scheduled Outages."
- (c) The deployment time will vary based on the specific requirements for Client's implementation.

4. Backups and Restoration

- (a) ISONAS will back-up the Software and all data hosted by it according to the backup and retention level and schedule specified in the Order Form for Hosting Services.
- (b) ISONAS will ensure that it has the capability to conduct a complete restoration (roll-back) of the Software and associated data from a backup;

5. Emergency upgrades or maintenance

- (a) If an emergency occurs ISONAS will take all necessary steps to avoid an Outage as a result of that emergency or the updates or maintenance required to resolve that emergency. An Outage caused by an emergency will be an Un-scheduled Outage.
- (b) If the only way to resolve the emergency is to install an Update or by conducting maintenance and this will cause an Outage, ISONAS will:
 - (i) notify Client immediately;
 - (ii) conduct any reasonable upgrades or maintenance as soon as possible within the standard maintenance windows or at another time agreed by Client; in cases of maximum severity, ISONAS may need to perform immediate upgrades or maintenance; and
 - (iii) take all reasonable steps to minimize the impact and length of any Outage.
- (c) An emergency means an actual or likely widespread security risk or imminent failure of the Software associated with not performing an Update or maintenance.

6. Monitoring and technical support

- (a) ISONAS will monitor the Hosting Services, the Software, all servers, operating systems, networks, server load, bandwidth, connectivity and network elements (**Monitored Elements**) 24 hours a day seven days a week by automated agents which will alert ISONAS’ on-call system administrators immediately if a fault arises.
- (b) ISONAS will ensure that its monitoring activities do not reduce or otherwise adversely impact availability.
- (c) ISONAS will use commercially reasonable efforts to maintain 98% Uptime as defined below:

7. System Availability: Upon mutual agreement between ISONAS and Client that the production environment is stable and has been approved by both parties for going live, The Hosting Services shall maintain a 99% Uptime level for Production Environments, which means that the Software will be accessible 99% of the time during any annual term, except as provided below.

“Uptime” percentage will be calculated per annual term, as follows:

$$\left[\left(\frac{\text{total} - \text{non-excluded}}{\text{total}} \right) * 100 \right] = \text{Uptime percentage}$$

- “total” constitutes the total number of minutes in the applicable annual term.
- An “Outage” of the Hosting Services is when no users can access the Software for more than 15 consecutive minutes.
- “non-excluded” constitutes the total number of minutes of an Outage during the applicable annual term that is not attributable to excluded events.

For any partial annual term covered by the Agreement, the Uptime percentage for that annual term will be calculated based on the total number of minutes in that annual term. Uptime percentage is tracked by ISONAS through a combination of monitoring packages. Upon request, ISONAS shall deliver to Client a report containing statistics on Uptime percentage within thirty (30) business days of the end of an annual term. Notwithstanding the foregoing, if Client requires an interim report, ISONAS will provide such report within one to three business days after request by Client.

Excluded Events: The occurrence of the following events are hereby excluded from ISONAS’ system availability guarantee under this Schedule:

- Planned downtime, which shall be any period for which ISONAS gives 8 hours or more notice that the Software will be unavailable.
- Force Majeure events (as defined in the Agreement).
- The inability of Client to access the Software due to internet, telecommunications, hardware, software, user error, or other issues outside the control of ISONAS.

General: Any obligations of ISONAS under this Schedule will be null and void upon any material breach by Client of the Agreement, including any failure by Client to meet payment obligations to ISONAS.