INSURANCE INFORMATION TECHNOLOGIES, INC. (“INSTEC”)
ACCEPTABLE USE POLICY

Instec has developed this Acceptable Use Policy (the "AUP") to establish the obligations of each end user client (the “Client”) using the Instec software and services on the hosted services (collectively, the “Services”), as set out in the applicable license agreement and order (the “Agreement”). Instec reserves the right to modify the AUP at any time. By using the Services, Client consents to be bound by the terms of this AUP. Insetec reserves right to interpret, apply, define and implement this AUP.

SUSPENSION, TERMINATION

If Instec determines, in its sole and reasonable discretion, that Client has violated this AUP, Instec may terminate or suspend its provision of the Services to Client. Instec will suspend the Service on the most limited basis as Instec determines is reasonably practical under the circumstances to address the underlying violation. Instec will attempt to notify Client prior to suspending the Services for violation of the AUP; provided, however, Instec may suspend service without notice if Instec becomes aware of a violation of any applicable laws, rules or regulations, including, but not limited, any activity that may expose Instec to criminal or civil liability or the Services to harm. Instec may take such further action as Instec determines to be appropriate under the circumstances to eliminate or preclude repeat violations, and Instec shall not be liable for any damages suffered by Client resulting in whole or in part from Instec 's exercise of its rights under this AUP.

TRADE AND EXPORT REGULATIONS; COMPLIANCE WITH LAW

The Services shall be used only for lawful purposes and shall not be used to transmit, distribute or store content in violation of any applicable laws, rules and regulations, including, without limitation, applicable trade and export regulations of the respective country in which the Services are utilized.

DATA PROTECTION

Client and Instec shall each comply with the Data Protection Schedule (“DPS”) set out in Exhibit 1, regarding the security and confidentiality of Client Data. In the event of a conflict between the DPS and the Agreement with respect to Client Data, the DPS shall control.

PROHIBITED CONDUCT

Inappropriate Content
Client shall not use the Services to transmit, distribute or store material that is inappropriate, as reasonably determined by Instec, or material that is obscene (including child pornography), defamatory, libelous, threatening, abusive, hateful, or excessively violent.

Intellectual Property
Material accessible through or contained within the Services may be subject to privacy, data protection or confidentiality laws and may contain intellectual property rights owned by Instec or third parties. Client shall not use the Services in any manner that would infringe, dilute, misappropriate, breach or otherwise violate any such intellectual property rights. Client shall ensure that all Client applications, software, programs, and content which are used with the Services are properly licensed and utilized.

Harmful Content
Client shall not use the Services to transmit, introduce, distribute or store material that may be harmful to or interfere with the Services or any third party's networks, systems, services, or web sites. Such prohibited harmful content includes, but is not limited to, viruses, worms, and trojan horses.

Fraudulent/Misleading Content
Client shall not use the Services to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims or representations.

Collecting Information
Client shall not use the Services to store or collect, or attempt to store or collect, personal data (including data as defined in the EU GDPR) without their prior knowledge and consent and Client must, as applicable, comply at all times with the EU GDPR and all other applicable data protection legislation.

Email and Unsolicited Messages
Client shall not use the Services to transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email ("spam"). Further, Client shall not use the service of another provider to send spam to promote a website hosted on or connected to the Services. In addition, Client shall not use the Services to send e-mail messages which are excessive and/or intended to harass or annoy other users.

Other Improper Actions
Client shall not use the Services to conduct activities that may be harmful to or interfere with the Services or any third party's networks, systems, services, or Web sites, including, but not limited to, flooding, mail bombing, or denial of service attacks.

Responsibility for Content
Instec assumes no responsibility for any content created or accessible on or through the Services unless it created such content. Instec is not obligated to monitor such content and will not exercise any editorial control over such content.

Reporting Violations
If Client becomes aware of a violation of this AUP, Client shall promptly report the violation to Instec by email to ____@instec.com

EXHIBIT 1

DATA PROTECTION SCHEDULE

1. COMPLIANCE WITH LAW AND DPS

Each party shall comply with all applicable data protection laws and regulations. Instec has implemented and maintains a written information security program. Except for compliance with applicable Data Privacy Laws, Instec shall not be responsible for providing any security or compliance controls unless agreed to in a SOW.

2. DATA PROCESSING AND CONTROL

2.1 *Client Data*

Instec shall: (A) take commercially reasonable steps to keep Client Data confidential in accordance with the Agreement; (B) not access any Client Data for any purpose other than as reasonably necessary to provide the Services, to exercise any right granted to it under the Agreement or as agreed to in writing by Client and Instec; and (C) require all personnel to comply with obligations consistent with the terms of this DPS.

2.2 *Legal Proceeding*

If Instec receives a request from a third party in connection with any government or court investigation or proceeding that Instec believes would require it to produce any Client Data, Instec shall, prior to producing or disclosing any such Client Data (if such notice is permissible according to applicable law), notify Client of such request, and reasonably cooperate with Client at Client's cost, if Client wishes to limit, challenge, or protect against such disclosure, to the extent permitted by applicable law or regulation.

3. DATA SECURITY / SECURITY INCIDENTS

3.1 *Services*

Instec shall implement and maintain in the Services, commercially reasonable and appropriate administrative, organizational, technical and physical measures to protect the security, integrity, confidentiality and availability of Client Data against unauthorized or unlawful access, use or disclosure. Notwithstanding anything to the contrary herein, in no event, shall Instec be held liable or responsible for any inaccuracies or omissions contained in, or the corruption of, any Client Data. Client shall be responsible for the encryption of Client Data to the Services.

3.2 *Security Incident*

If Instec becomes aware of a security incident that impacts Client Data, Instec shall promptly notify Client of the security incident and shall, subject to applicable laws, regulations, or a governmental request, provide Client with details to the extent available about the security incident, including, how it occurred and to the extent caused by a breach of Instec of its obligations under this DPS, how Instec will address the security incident. In the event of a security incident, Instec and Client shall cooperate in good faith to resolve any privacy or data security issues involving Client Data, and to make any legally required notifications to individuals affected by the security incident, subject to the Agreement. Notwithstanding anything to the contrary, Instec shall have no liability for any security incident to the extent the applicable Client Data was not encrypted and such security incident did not solely result from a breach by Instec of its obligations under this DPS or the Agreement.

3.3 *Third Party Notice*

Except as otherwise required by applicable law or regulation, Instec shall not inform any third party of any security incident without first obtaining Client's prior written consent, other than to inform a complainant that the matter has been forwarded to Client. The parties shall work together in good faith on the content of any notification of a Security Incident.

4. DATA PROTECTION TRAINING.

Instec shall require personnel who have access to Client Data to complete privacy and data security training on a periodic basis in accordance with its standard employment policies.

5. DATA SECURITY INSPECTIONS AND AUDITS.

Instec shall provide Client with information as may be reasonably requested by Client from time to time regarding Instec's compliance with its data security obligations under this DPS, provided that disclosure of any such information would not violate Instec's reasonable privacy or data security policies, or confidentiality obligations with any third party.

6. TERMINATION / RETURN OR DESTRUCTION OF CLIENT DATA.

This DPS shall terminate when the Agreement terminates or expires. Upon such termination, Client shall be responsible for removing or deleting Client Data from the Services; provided, however, at Client's sole cost and expense and subject to a statement of work entered into by the parties, Instec may assist Client with the removal of the Client Data and provide certification or proof of removal. Following termination, Instec shall have no liability for the Client Data.