DATA PROCESSING AGREEMENT

When Customer renews or purchases a new subscription subject to the General Terms and Conditions, the then-current DPA will apply and will not change during Customer's subscription for that General Terms and Conditions, except 1) RIB has introduces features, supplements or related software that were not previously included with the subscription, in such case, RIB may provide terms or make updates to the DPA that apply to Customer's use of those new features, supplements or related software, or 2) any current or future government requirement or obligation in any country that cause RIB believe the provisions of the DPA that may conflict with any governmental requirement or obligation, in such case, RIB may provide terms or make updates to the DPA that apply to such country.

Capitalized terms used but not defined in this DPA will have the meanings provided in the General Terms and Conditions.

1. Basis for the Data Processing Agreement ("DPA")

(a) This agreement lays down the rights and obligations that apply when the Processor [**RIB**] processes personal data on behalf of the Controller [the **Customer**].

(b) The agreement has been drawn up with a view to compliance by the parties with applicable data protection law that generally applicable to information technology service providers, especially the Article 28(3) of ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation", or "GDPR")*** that sets specific requirements concerning the content of a data processing agreement.

(c) Controller must comply with all laws and regulations applicable to its use of Application, including laws related to confidentiality of communications, and applicable data protection law. Controller is responsible for determining whether the Application is appropriate for storage and processing of information subject to any specific law or regulation and for using the Application in a manner consistent with Controller's legal and regulatory obligations. Controller is responsible for responding to any request from a third-party regarding Controller's use of the Application.

(d) The duration of the processing depends on the duration of the main contract.

(e) The nature and purpose of the processing, as well as the type of personal data and categories of data subjects are specified in Schedule 2.

2. The Processor acts on instructions

(a) The Processor processes personal data on documented instructions from the Controller, unless required to do so by applicable data protection law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; see Article 28(3)(a) of GDPR.

(b) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the applicable data protection law.

(c) Unless otherwise specified in the General Terms and Conditions, Controller may not provide Processor with any sensitive or special personal data that imposes specific data security or data protection obligations on processer in addition to or different from those specified in the DPA or General Terms and Conditions.

3. Confidentiality

(a) The Processor ensures that the persons authorised to process personal data on behalf of the Controller have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Security of processing

(a) The Processor takes all measures required pursuant to Article 32 of the GDPR. Details of the Information Security Requirement see Schedule 3.

5. Engagement of sub-processors

(a) The Processor can engage other processors ("sub-processors") for the performance of the data processing agreement. These sub-processors will be accessible on the Processor's website.

(b) The Processor will inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Controller the opportunity to object to such changes. Where the Controller chooses to object to these changes, the Controller has every right to rescind the agreement prospectively.

(c) The Processor informs the Controller of the above changes by updating the list of sub-processor on the website one month before the change of sub-processors will take place. The Processor will also send an e-mail and inform the Controller's representative (the person who has signed the agreement) if the list of sub-processors on the Processor's website has been changed.

(d) The Processor will make sure that the same data protection obligations are imposed on sub-processors as those laid down in this data processing agreement via a contract or other legal act under Union or Member State law whereby in particular the appropriate safeguards are provided that the sub-processor will take the necessary technical and organisational measures in such a manner that the processing complies with the requirements of the data protection regulation.

(e) Where the sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

6. Transfer of personal data to third countries or international organisations

(a) Processor shall be entitled to process Personal Data, including by using sub-processors, in accordance with this DPA outside the country in which the Controller is located as permitted under applicable data protection law.
(b) Standard Contractual Clauses, see Schedule 1:
    a. Where (i) personal data of an European Economic Area ("EEA"), or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) personal data of another controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then: (a) Processor and Controller enter into the Standard Contractual Clauses;
    b. Controller joins the Standard Contractual Clauses entered into by Processor and the sub-processor as an independent owner of rights and obligations; and/or
    c. Other Controllers whose use of the Application has been authorized by Controller under the Agreement may also enter into Standard Contractual Clauses with Processor and/or the relevant sub-processors in the same manner as Controller in accordance with Sections 6 (b) above. In such case, Controller will enter into the Standard Contractual Clauses on behalf of the other Controllers.
(c) Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and sub-processor rules in Sections 9, such specifications also apply in relation to the Standard Contractual Clauses.
(d) The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

7. Assistance to the Controller

(a) Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the data protection regulation.

(b) The Processor assists the Controller in ensuring compliance with the Controller's obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor; see Article 28(3)(f) of GDPR.

(c) The processor will immediately inform the controller of any violation of the protection of personal data of which he becomes aware.

8. Erasure

(a) The Processor can remove a user, but the traces a user has left (the user's log information) cannot be deleted as they serve the purposes of the platform and are a condition for the correct and documented use of the RIB products by others.

9. Monitoring and audits

(a) The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and this agreement and allows and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller only if:
    a. There has sufficient evidence that Processor failed its compliance with the technical and organizational measures that protect the production systems of the Application;
    b. A personal Data Breach has occurred;
    c. An audit is formally requested by Controller's data protection authority; or
    d. Mandatory applicable data protection law provides Controller with a direct audit right and provided that Controller shall only audit once in any twelve month period unless mandatory applicable data protection law requires more frequent audits.

(b) Controller shall provide at least sixty days advance notice of any audit unless applicable mandatory data protection law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Controller audits shall be limited in time to a maximum of two business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Controller shall provide the results of any audit to Processor.

(c) Controller shall bear the costs of any audit unless such audit reveals a material breach by Processor of this DPA, then Processor shall bear its own expenses of an audit. If an audit determines that Processor has breached its obligations under the DPA, Processor will promptly remedy the breach at its own cost.

10. California Consumer Privacy Act ("CCPA")

(a) If Processor is processing personal data within the scope of the CCPA, Processor makes the following additional commitments to Controller. Processor will process Customer Data and personal data on behalf of Controller and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Processor sell any such data. These CCPA terms do not limit or reduce any data protection commitments Processor makes to Controller in the DPA, General Terms and Conditions, or other agreement between Processor and Controller.

11. Changes and the notification obligation of the Controller

(a) If a person signs this DPA on behalf of the Controller that person will be regarded as the "representative of the Controller" and information on any changes to the data processing agreement will be submitted to the representative.

(b) It is the obligation of the Controller to notify the Processor if the "representative of the Controller" is changed or the contact information of the representative changes.

12. Deletion and return

(a) Upon termination of the processing services, the processor shall, at the choice of the controller, either delete or return all personal data, as well as documents, other data and generated processing or usage results relating to the contractual relationship, unless there is an obligation to store or retain them under Union or national law.The processor's data shall be irretrievably deleted in accordance with data protection law. An irrevocable physical deletion shall be recorded. This also applies to any data backups at the processor. The processor shall document the deletion in a suitable manner. If there are legal storage obligations, the data must be deleted after the end of the storage obligation. An appropriate deletion concept shall be documented.

(b) Prior to the termination of the contractual services, the processor may only delete data that are no longer required with the prior consent of the responsible party. Consent to deletion can also be given by agreement of the contractual parties to a deletion concept.

Schedule 1 STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer also on behalf of the other Controllers

(the data exporter)

And

RIB

(the data importer)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Schedule 2.

Clause 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;

(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 his behalf after the transfer in accordance with his 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 his 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 organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Schedule 2 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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.

4. 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.

Clause 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 organisational security measures specified in Schedule 3 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, unauthorised 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 Schedule 3, 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 subject as the data importer under the Clauses; and

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

Clause 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 organisational security measures specified in Schedule 3 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 unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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 Schedule 3 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;

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

Clause 6

Liability

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.

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 his 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 of 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.

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.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

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.

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).

Clause 9

Governing law

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

Clause 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 Clause.

Clause 11

Sub-processing

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 (1). 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.

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.

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.

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.

Clause 12

Obligation after the termination of personal data-processing services

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.

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.

Schedule 2 to the DPA and, if applicable, the Standard Contractual Clauses

Data exporter

Customer is the data exporter. The data exporter is a user of Application or Professional Services.

Data importer

The data importer is RIB, a global producer of software and services.

Data subjects

The persons in the Customer's enterprise

Categories of data

The personal data transferred concern the following categories of data:

- Full name
- Name of organisation/enterprise
- E-mail address
- The activities of users in RIB's products
    - In addition to this, the user may when signing up for RIB's products himself/herself actively choose to complete information concerning the following:
- Title
- Initials
- Tel. no./mobile tel. no.
- Department

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

As set out in the General Terms and Conditions (including the Quote) if any.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Collects and registers personal data when persons in the enterprise of the controller sign up for RIB's products. The processor uses the data collected only to carry on the business and deliver the products offered by the enterprise. That means that the processor uses the data e.g. to improve the user experience and to adapt the products. Data may also be used to communicate with the customer, e.g. to inform the customer of security conditions and product information.

Duration of the processing

The processing is not for a fixed term and goes on until the data processing agreement is terminated or rescinded prospectively by one of the parties.

Schedule 3 to the DPA and, if applicable, the Standard Contractual Clauses - Technical and Organizational Measures

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Safeguards. RIB at all times shall maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, availability, and integrity of (i) Customer's Confidential Information that it maintains or transmits and (ii) logon credentials and computing equipment and devices used, or capable of being used, for remote access to any network or system that is operated by or on behalf of Customer.

2. Secure Destruction. When required under this Agreement and in any case when any of Customer's Confidential Information is no longer needed by RIB to perform the Services, the media on which such Confidential Information is stored or recorded shall be destroyed as follows: (i) paper, film, or other hard copy media shall be shredded or destroyed such that the Confidential Information cannot be read or otherwise cannot be reconstructed; and (ii) electronic media shall be cleared, purged, or destroyed consistent with NIST Special Publication 800 88, Guidelines for Media Sanitization, such that the Customer's Confidential Information cannot be retrieved.

3. Subcontractors. Any disclosure of Customer's Confidential Information to an independent contractor or agent of RIB Subcontractor (each, a "**RIB Subcontractor**") shall be pursuant to a written agreement between RIB and such RIB Subcontractor containing restrictions and conditions on the use and disclosure of Customer's Confidential Information intended to provide the safeguards contemplated in Section **Error! Reference source not found.** of this Schedule. RIB shall take reasonable steps to ensure that the acts or omissions of its RIB Subcontractors would not breach the terms of the Agreement if done by RIB, including making reasonable inquiry of such RIB Subcontractors regarding their ability to comply with the foregoing obligations and taking reasonable steps to monitor such compliance.

4. Security Incident. RIB shall report to Customer in writing any Security Incident (as hereinafter defined) involving or materially threatening Customer's Confidential Information, other than a Security Incident that involves an actual or reasonably suspected Data Breach reported pursuant to Section 7 of this Scheudle, within 30 days of RIB's discovery thereof. For purposes hereof, "Security Incident" means (i) the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information that is maintained in or processed, transmitted, or received a facility at which RIB or any RIB Subcontractor provides services pursuant to the Agreement or (ii) the interference with system operations of the foregoing, in each case other than events that are trivial, routine, do not constitute a material threat to the security of such information, and do not result in unauthorized access to or use or disclosure of such information (such as typical pings and port scans).

5. Encryption of PII.

    a. "***PII***" means Customer's Confidential Information that (i) is personally-identifiable information of an individual, (ii) reasonably might be used (alone or in combination with other information) to identify an individual or to obtain personally-identifiable information of an individual, or (iii) the unauthorized use or disclosure of which would violate any law or regulation or would give rise to an obligation of notification to such individual or any governmental body.

    b. RIB shall render all Customer Data and any PII in transmission unusable, unreadable, or indecipherable by encryption using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Such algorithmic process shall comply with the requirements of Federal Information Processing Standards (FIPS) 140 2, Security Requirements for Cryptographic Modules, including, as appropriate, standards described in NIST Special Publication 800 52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800 77, Guide to IPsec VPNs, NIST Special Publication 800 113, Guide to SSL VPNs, or other standards that are FIPS 140 2 validated.

    c. With regard to Customer Data and PII stored on laptop computers, mobile devices, external hard drives, and removable media, RIB shall, and with respect to PII otherwise stored RIB shall use reasonable efforts to, render all PII in storage unusable, unreadable, or indecipherable by encryption using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Such algorithmic process shall be consistent with the National Institute of Standards and

Technology (NIST) Special Publication 800 111, Guide to Storage Encryption Technologies for End User Devices.

6. Data Breach.

   a. "**Data Breach**" means any use or disclosure of Customer's Confidential Information not expressly authorized under, or in breach of, the terms and conditions of the Agreement or in violation of applicable law.

   b. Without unreasonable delay and in no case later than 10 days after discovery of an actual or reasonably suspected Data Breach, RIB shall notify Customer of an actual or reasonably suspected Data Breach, such notice to describe the circumstances of the Data Breach, including without limitation, to the extent known, (i) a brief description of what happened, including the date of the Data Breach and the date of the discovery of the Data Breach, (ii) a description of the types of data that were involved in the Data Breach, and (iii) a brief description of what RIB is doing to investigate the Data Breach, to mitigate harm from the Data Breach, and to protect against any further Data Breaches.

   c. RIB shall conduct such further investigation and analysis as is reasonably required or reasonably requested by Customer and promptly shall advise Customer of additional information pertinent to the Data Breach that RIB obtains.

   d. For purposes hereof, an actual or reasonably suspected Data Breach shall be deemed discovered by RIB as of the first day on which such actual or reasonably suspected impermissible use or disclosure is known to RIB or, by exercising reasonable diligence, would have been known to RIB, and RIB shall be deemed to have knowledge of an impermissible use or disclosure if such impermissible use or disclosure is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the impermissible use or disclosure) who is an employee, agent, or independent contractor of RIB.

   e. RIB shall take all actions reasonably necessary, and shall cooperate with Customer as reasonably requested, to mitigate, to the extent practicable, any harmful effect of a Data Breach.

7. Third-party Reports.

   a. In the event that RIB obtains any third-party assessment of the design and/or effectiveness of its information security management program (such as, without limitation, a SOC 2 report prepared by a Certified Public Accountant) or achieves any third-party certification of its information security management program (such as, without limitation, certification under ISO 27001), RIB promptly thereupon shall deliver to Customer a copy of such assessment report or certificate or, at RIB's election, notify Customer thereof and permit Customer or, subject to the execution of a confidentiality and security agreement reasonably acceptable to RIB, Customer's designee to review the same at RIB's offices or via a secure online collaboration session).

   b. Any such report delivered pursuant to this section will be deemed the Confidential Information of RIB.

   c. If any such report includes any findings that RIB materially fails to comply with the applicable standards or includes any material test exceptions, RIB shall use reasonable efforts to remedy such noncompliance promptly. If RIB fails to deliver to Customer evidence of such remedy reasonably satisfactory to Customer within 45 days following such report, or if RIB fails to provide any report or certificate when required pursuant to this paragraph, then any provision of this Agreement to the contrary notwithstanding, Customer may terminate this Agreement without penalty upon written notice to RIB given any time thereafter until such evidence or such report or certificate (as the case may be) is so delivered.

8. Cyber Insurance.

   a. RIB shall procure and maintain, at its sole expense, from an insurance company having an A.M. Best rating of "A-" or better and with a financial size category of at least Class VII or, if such ratings are no longer available, with comparable ratings from a generally recognized insurance rating agency, insurance coverage for the unauthorized acquisition, access, use, physical taking, release, distribution, or disclosure of personal information, identity theft, and breaches by third parties and employees, for costs and expenses arising from or relating to an unauthorized disclosure or use of Customer Data or any use or disclosure of Customer Data in breach of the terms and conditions of this Agreement or in violation of applicable law, including such costs and expenses of notification, fraud alert and credit monitoring, mitigation of damages, consultants, forensic investigation, and legal expenses, such policy to include, at a minimum, (A) third-party coverage for data privacy and computer network security breaches, internet and electronic media liability, and professional

services liability, (B) first-party business interruption coverage in the event of a network security breach, (C) first-party cyber extortion coverage for threats against data and identity theft, (E) liability coverage for claims related to computer viruses or other malicious code, (F) liability coverage for claims related to theft or destruction of data, and (G) reimbursement for expenses notification of, and costs associated with credit monitoring for, parties affected by a security breach, costs for investigating and managing a security breach, and data privacy regulatory fines and penalties, with limits of not less than $5,000,000 as an annual aggregate ("**Cyber Insurance**").

b. Upon its procurement of the foregoing insurance and thereafter upon Customer's request from time to time, and upon any replacement of or material change to any policy required under this Agreement, RIB shall furnish Customer with certificates or other proof of each such policy reasonably satisfactory to Customer. RIB shall notify Customer within three business days following any cancellation, or receipt of notice of cancellation, of any such policy.

c. The requirements as to the types and limits of insurance coverage to be maintained by RIB pursuant to this Agreement, and any approval or waiver of said insurance by Customer, is not intended to, and shall not, limit or qualify in any manner the liabilities and obligations otherwise assumed by RIB pursuant to this Agreement, including without limitation provisions relating to indemnification. The procurement and maintenance of insurance required under this Agreement shall not limit or affect any liability that RIB may have by virtue of this Agreement or otherwise.