Information Security Requirements Agreement 14/Nov/2022 v1.4

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, by RIB for remote access to any network or system that is operated by or on behalf of Customer. Those safeguards will include, but are not limited to, measures designed to prevent unauthorised access to or disclosure of Confidential Information (other than by Customer or Customer Users).

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, RIB will take reasonable steps to ensure the Confidential Information is (at RIB's discretion) permanently destroyed, de-identified, deleted or put beyond use, in accordance with applicable data protection law. In this paragraph, "put beyond use" means that RIB: (i) is not able, or will not attempt, to use the Confidential Information for any purpose; (ii) does not give any other organisation access to the Confidential Information; (iii) surrounds the Confidential Information with appropriate technical and organisational security measures; and (iv) commits to permanent deletion of the Confidential Information if, or when, this becomes possible.

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 that provides the safeguards required in Section 1 of this Agreement. 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 6 of this Schedule, within 10 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 loss, 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 access, use or disclosure of Customer's Confidential Information or Personal Information not authorized under, or in breach of, the terms and conditions of the Agreement or in violation of Privacy Laws.

(b) Without unreasonable delay and in no case later than 3 days after RIB becomes aware 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) 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.