TECHNOLOGY LICENSE TERMS

Last modified: 1 December 2025 (v 2.1)

These TECHNOLOGY LICENSE TERMS ("**Agreement**") govern your access to and use of the Licensed Product (as defined below), and constitute a legally binding agreement between you (whether an individual, corporation, or other entity) ("**Client**") and RWS, where RWS is commissioned by Client to provide the Licensed Product as further detailed in the applicable Order Form. The RWS legal entity providing the Licensed Product and entering into this Agreement ("**RWS**") shall be the entity expressly identified as such in the applicable Order Form. If no such entity is specified in the Order Form, RWS shall be deemed to be the entity that issued or signed the Order Form. By registering, subscribing, purchasing, or otherwise using the Licensed Product, or accepting this Agreement (acceptance is made by clicking on the box that means acceptance, entering a software encryption code, or signing an Order Form referring to this Agreement), you agree to be bound by the terms of this Agreement. If you do not agree with the terms of this Agreement, you must not use the Licensed Product.

RWS reserves the right to amend or update this Agreement at any time, in its sole discretion. Any changes will be effective immediately upon posting on the RWS website and it is the responsibility of the Client to review the Agreement regularly to stay informed of any updates. The version of the Agreement applicable to you will be the version in effect on the date of your Order Form, unless otherwise agreed in writing.

IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. LICENSED PRODUCT QUANTITIES, DESCRIPTIONS, PURCHASED OPTIONS AND NUMBER OF USER(S) WILL BE DEFINED IN AN ORDER FORM OR OTHER VALID FORM OF AGREEMENT ACKNOWLEDGED IN WRITING BY RWS OR THE PARTY WHO PROVIDED THIS LICENSED PRODUCT TO YOU ("**ORDER FORM**"). IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT ACCESS, OR USE THE LICENSED PRODUCT AND PROMPTLY RETURN THE UNUSED LICENSED PRODUCT TO THE PARTY FROM WHOM YOU OBTAINED THE LICENSED PRODUCT.

Article 1. Definitions

1.1 ***"Affiliates"*** means an entity controlled by a party. The word "**control**" shall, in the context of a corporation, mean direct beneficial ownership of at least fifty per cent (50%) of the shares entitled to vote for members of the Board of Directors of such corporation, and, in the context of any other business entity, shall mean the right to exercise similar management and control over such entity.

1.2 ***"Confidential Information"*** means all information, including but not limited to this Agreement, its terms, pricing, and Fees; the Licensed Product and Documentation; reports, analyses, summaries, and outputs; and any information, data, materials, or content disclosed by either party to the other, whether directly or indirectly, in writing, orally, electronically, or by inspection of tangible objects (including documents and equipment), that is (i) marked or identified as confidential or proprietary, or (ii) not so

marked but which, given its nature or the circumstances of disclosure, would reasonably be understood to be confidential or proprietary, or the disclosure of which could reasonably be expected to cause competitive harm to the owner of such information.

1.3 ***"Content"*** means any information or material that is provided to RWS in connection with Client's use of the Licensed Product, including but not limited to, files, pages, data, works such as video clips, audio clips, metatags or images.

1.4 ***"Documentation"*** means the manuals and other technical and functional documentation provided by RWS to Client for use with the Licensed Product.

1.5 ***"Fees"*** means the fees for the Licensed Product and related Support Services as specified in the relevant Order Form.

1.6 ***"Intellectual Property Rights"*** means patent rights (including patent applications and disclosures), copyrights, trademarks, trade secrets, know-how and any other intellectual property rights recognized in any country which is a party to the Berne Convention.

1.7 ***"Licensed Product"*** means the software products as specified in the relevant Order Form or any addendum thereto, made available either in object code form or on-line by RWS from time to time.

1.8 ***"Service Catalogue"*** means the document that describes in detail the level of service including uptime and availability to be provided by RWS in relation to the Licensed Product.

1.9 ***"Support"*** means the technical support service more particularly set forth in Article 9 which is to be provided by RWS to Client.

1.10 ***"Term"*** has the meaning set forth in the relevant Order Form.

1.11 ***"Support Level"*** means the Support package purchased by the Client as detailed under the Order Form.

1.12 ***"Third Party Software"*** means the software programs designated in the relevant Order Form as a third-party software program.

2. License Grant and Restrictions

2.1 ***License.*** Subject to the terms and conditions of this Agreement, RWS grants Client a non-exclusive, non-sublicensable, non-transferable, limited license to use the Licensed Product and Documentation, limited to the terms of the relevant Order Form, and only for Client's internal use. Except for archival purposes, Client may not use or store any copies of the Licensed Product unless expressly authorized in writing by RWS in the applicable Order Form. RWS reserves all rights and licenses in and to the Licensed Product not expressly granted to Client under this Agreement.

2.2 ***Third Party Software.*** In the event that there is any Third Party Software provided by RWS to Client under an Order Form, such Third Party Software shall be governed by the license agreement provided by the licensor of such Third Party Software.

2.3 ***Client Feedback and Product Enhancement.*** Client grants RWS and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Licensed

Product any suggestions, enhancements, recommendations or other feedback provided by Client relating to the operation of the Licensed Products. RWS solely for the purpose of enhancement and development of its products reserves the right to deploy telemetry software to record the nature of use and performance of the product through collection of anonymous usage data.

2.4 ***Client Feedback and Product Enhancement.*** Client grants RWS and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Licensed Product any suggestions, enhancements, recommendations or other feedback provided by Client relating to the operation of the Licensed Products. RWS solely for the purpose of enhancement and development of its products reserves the right to deploy telemetry software to record the nature of use and performance of the product through collection of anonymous usage data.

Article 3. Restrictions

3.1 Client shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Licensed Product, and shall notify RWS promptly of any such unauthorized use. Client shall not transmit any data that it has reason to believe is infringing, obscene, threatening, libelous, or otherwise unlawful or tortious, including material harmful to children or violative of third-party privacy rights, and Client shall indemnify and defend RWS from and against any breach of the foregoing restriction. In addition, Client shall not (a) copy, reproduce, distribute, republish, download display, post or transmit in any form or means the Licensed Product or the Documentation, (b) rent, transfer, lease, loan, resell for profit or otherwise, distribute, or otherwise grant any rights in the Licensed Product in any form to any other party in whole or in part, including without limitation to provide processing services to their parties for commercial timesharing or for rental or sharing arrangements, (c) modify, adapt, decompile, disassemble, reverse engineer, create derivative works or otherwise attempt to derive source code from the Licensed Product (or hosting environment, if applicable) in whole or in part, (d) or remove, modify, obscure and/or otherwise deface any copyright, trademark or other proprietary rights notices in the Licensed Product or Documentation.

Article 4. Payments and Audit Rights

4.1 ***Fees.*** Unless otherwise agreed in a relevant Order Form all Fees will be defined and payable in accordance with the applicable Order Form. All Fees will be due and payable within thirty (30) days from the date of RWS's invoice. All Fees are stated and payable in the currency detailed in the relevant Order Form. All Fees are non-cancellable and non-refundable.

4.2 ***Interest.*** Except for any amounts disputed in good faith, all past due amounts will incur interest at a rate of 1.5% per month or the maximum rate permitted by law, whichever is less. Client will reimburse RWS for all reasonable costs and expenses incurred (including reasonable attorneys' fees) in collecting any overdue amounts.

4.3 ***Taxes.*** All Fees set forth in the applicable Order Form are exclusive of any sales, withholding taxes, value-added, or other similar taxes imposed by applicable law that RWS must pay based on the Licensed Product and related services ("**Taxes**"). Client agrees to pay or reimburse RWS for all such relevant taxes, except for taxes based on RWS's income (which shall be the responsibility of RWS). If RWS has the legal obligation to pay or collect Taxes for which Client is

responsible under this Section. Client will pay that amount unless Client can provide RWS with a valid tax exemption certificate authorized by the appropriate taxing authority.

4.4 ***Renewals.*** RWS may increase the fees for the Licensed Product / Support by not more than the higher of five percent (5%) and the Consumer Price Index (CPI) applicable in the jurisdiction defined in Section 16.2, in any subsequent renewal term, as set forth in the relevant Order Form.

4.5 ***Reporting and Audit.*** Client shall keep complete and accurate books and records of its use of the Licensed Product to demonstrate its compliance with this Agreement. Further, RWS may audit Client's use of the Licensed Product in order to verify compliance with this Agreement. An audit shall occur no more frequently than once annually at RWS's expense. All audits shall be conducted during regular business hours and shall not unreasonably interfere with Client's business activities. RWS shall schedule any audit at least thirty (30) days in advance. If any audit by RWS yields any deficiency in the amounts that should have been paid to RWS, Client shall promptly remit payment to RWS of such amounts plus interest calculated at a rate of 1.5% per month from the date on which such payment became due or the highest rate permitted by law, whichever is lower. In addition, if an audit by RWS yields a deficiency of 5% or more in the amounts that should have been paid to RWS, Client will promptly reimburse RWS for all reasonable costs of the audit.

Article 5. Term and Termination

5.1 ***Agreement.*** The term of this Agreement shall commence on the execution of a relevant Order Form Effective Date and shall continue in effect through the License Term set forth in the applicable Order Form, unless and until this Agreement is terminated in accordance with this Section 5. Unless otherwise agreed to in the relevant Order Form, the Order Form will automatically renew for all available offerings at the end of the initial Term (or any renewal Term thereafter) for additional one (1) year periods, unless Client has provided RWS with a written termination notice of its intention not to renew the relevant Order Form and/or Agreement at least sixty (60) days prior to the expiration of the then current Term.

5.2 ***Termination.*** This Agreement, including all licenses granted hereunder, may be terminated as follows: (a) by either party with immediate effect if the other party fails to perform any of its material obligations under this Agreement and such failure continues for thirty (30) days after receipt of written notice; (b) by either party with immediate effect upon written notice in the event that the other party: (i) becomes insolvent; (ii) makes an assignment for the benefit of creditors; (iii) files a voluntary bankruptcy petition; (iv) acquiesces to any involuntary bankruptcy petition; (v) is adjudicated bankrupt; or (vi) ceases to do business; or (c) by RWS immediately upon written notice of termination in the event of any breach of Section 2 (Grant of License).

5.3 ***Effect of Termination.*** Upon the expiration or termination of this Agreement, Client shall immediately cease use of the Licensed Product or Support and each party shall immediately cease use of the Confidential Information of the other party, and each party shall return or, at its option, destroy the materials referred to in the foregoing sentence from all equipment and electronic and other media, including all copies thereof. Each party shall certify in writing its compliance with the foregoing upon the request of the other party.

5.4 ***Survival.*** The rights and obligations of the parties which by their nature extend beyond the expiration or termination of the Agreement shall survive termination or expiry of this Agreement for any reason.

Article 6. Warranties

6.1 ***Limited Warranty.***

6.1.1 ***For On Premise Licensed Products:*** RWS warrants to Client that, for a period of ninety (90) days from the effective date of the applicable Order Form (the "Warranty Period"); the Licensed Product delivered pursuant to such Order Form will substantially perform in accordance with the Documentation.

6.1.2 ***For Cloud based Licensed Products***: RWS warrants that, for the Term of the applicable Order Form ("Warranty Period") that the Licensed Products will substantially conform in accordance with Documentation. The foregoing warranty shall not apply if the Licensed Product has not been properly used at all times in accordance with the Documentation.

6.2 ***Sole Remedy.*** If the Licensed Product fails to perform substantially in accordance with the Documentation, Client must notify RWS in writing within the Warranty Period. As Client's sole and exclusive remedy and RWS's entire liability for any breach of the warranty set forth in this Section, RWS will, at its option: (a) promptly correct any Licensed Product that fails to meet this warranty; (b) provide Client with a reasonable procedure to circumvent the nonconformity; or if RWS determines that options (a) or (b) are not commercially feasible, then (c) terminate the affected Order Form and refund to Client the Fees actually paid by Client for the affected Licensed Product under that Order Form during the twelve (12) month period immediately preceding the date on which Client first notified RWS of the warranty breach.

6.3 The warranty set herein shall not apply to Licensed Products which are On Premise if: (i) the Licensed Product has not been properly installed or used at all times in accordance with the Documentation and supported platforms; (ii) Client (either itself or via a third party on its behalf) has modified the Licensed Product; (iii) Client has combined the Licensed Product with other software or hardware not provided or approved by RWS pursuant to the documentation; or (iv) the Licensed Product has been subject to misuse, neglect or unusual physical, electrical or electromagnetic stress, or some other type of accident, other than where it was in RWS's reasonable control to prevent such an occurrence.

6.4 ***Disclaimer.*** RWS does not warrant that the Licensed Product will meet Client's requirements, that the operation of the Licensed Product will be error-free, timely or the operation therefore will be uninterrupted or that all Licensed Product errors will be corrected. EXCEPT AS PROVIDED IN SECTION 6.1, THE LICENSED PRODUCT HEREUNDER ARE PROVIDED "AS IS" AND RWS MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE LICENSED PRODUCT OTHER THAN THAT THE LICENSED PRODUCT WILL CONTINUE TO MEET THE DOCUMENTATION. RWS DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE. No advice or information, whether oral or written, obtained from RWS or elsewhere will create any warranty not expressly stated in this Agreement.

6.5 ***Compliance.***

6.5.1 ***Fraud.*** Client represents and warrants that neither it nor any of its officers, directors, employees, agents, contractors, or representatives has engaged, or will engage, in any act of fraud, intentional misrepresentation, deception, or other fraudulent conduct in connection with this Agreement or the performance of any obligations hereunder.

6.5.2 ***Sanctions.*** The Client represents and warrants that, at the time of entering into the Order Form and this Agreement, and throughout the term of the Order Form and this Agreement, (i) it is not listed on the Specially Designated Nationals and Blocked Persons Lists maintained by the Office of Foreign Assets Controls (OFAC), and (ii) it is not subject to any sanctions, embargoes or restrictions imposed by any governmental or regulatory authority, including but not limited to those imposed by the United Nations, the United Kingdom, the United States, the European Union or any other relevant authority. The Client shall promptly notify RWS if it becomes subject to any sanctions, embargoes or restrictions during the Term of the Order Form and this Agreement.

6.5.3. ***Export.*** Client agrees to comply fully with all applicable export laws and regulations of the United States and other jurisdictions to ensure that neither the Licensed Product, nor any direct product thereof are exported or re-exported in violation of such laws or used for any purposes prohibited by such laws. The Licensed Product is "commercial computer software" or "commercial computer software documentation."

6.6 ***Acceptable Use Policy***. Client acknowledges that neither RWS nor its suppliers or licensors exercise any control over the Content provided by Client when using the Licensed Product, and that it is the sole responsibility of the Client that such information complies with the Acceptable Use Policy set forth in Exhibit A (Acceptable Use Policy).

6.7 ***Service Catalogue.*** Licensed Products will be provided to Client in accordance with the relevant section of RWS's relevant Service Catalogue.

Article 7. Limitation of Liability

7.1 IN NO EVENT SHALL EITHER PARTY, ITS DIRECTORS, OR EMPLOYEES BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON CONTRACT, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY, HOWEVER CAUSED AND WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE, KNOWN, FORESEEN, OR A PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. RWS's total cumulative liability under this Agreement shall not exceed the amount of the fees paid by Client for the Licensed Product and Support Services, as applicable, during the preceding twelve (12) months which gave rise to a claim.

7.2 The parties acknowledge that these limitations and exclusions of liability are agreed to be reasonable allocations of liability and risk, having considered the relative commercial size of the parties, the nature of the contractual obligations, the ability of the parties to bear the losses and the availability of insurance.

Article 8. Infringement Claims

8.1 ***Infringement Indemnity.*** Subject to Client's compliance with the terms and conditions of this Agreement, RWS will, at its option, defend or settle any action brought against Client to the extent that it is based upon a third party claim that the Licensed Product, as provided by RWS to Client under this Agreement and used within the scope of this Agreement, infringes any Intellectual Property Rights, and will pay any costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against Client, provided that Client: (a) promptly notifies RWS in writing of the claim; (b) grants RWS sole control of the defense and settlement of the claim; and (c) provides RWS, at RWS's expense, with all assistance, information and authority reasonably required for the defense or settlement of the claim.

8.2 ***Injunctions.*** If Client's use of any of the Licensed Product hereunder is, or in RWS's opinion is likely to be, enjoined due to the type of claim specified in Section 8.1 above, RWS may, at its sole option and expense: (a) procure for Client the right to continue using such Licensed Product under the terms and conditions of this Agreement; (b) replace or modify such Licensed Product so that it is non-infringing and substantially equivalent in function to the enjoined Licensed Product; or (c) if options (a) and (b) above cannot be accomplished despite RWS's commercially reasonable efforts, then RWS may terminate Client's rights and RWS's obligations hereunder with respect to such Licensed Product and refund to Client the amount of fees paid to RWS for the Licensed Product less an amount for depreciation determined on a straight-line four year depreciation basis with a commencement date as of the effective date of the respective Order Form.

8.3 ***Exclusions.*** Notwithstanding Section 8.1, RWS will have no liability for any infringement or misappropriation claim of any kind to the extent that it results from (a) Client's operation, combination or use of the Licensed Product with equipment, devices, software or data not supplied by RWS, if a claim would not have occurred but for operation, combination or use; (b) Client's use of the Licensed Product other than in accordance with this Agreement or the Documentation; (c) modifications of a Licensed Product by anyone other than RWS where the unmodified version of the Licensed Product would not be infringing; (d) use by users or Affiliates of Client not permitted by this Agreement; or (e) Client uses a version of the Licensed Product which has been superseded and/or is no longer supported by RWS, if the claim could have been avoided by using the current version of the Licensed Product.

8.4 ***Sole Remedy.*** THE PROVISIONS OF THIS SECTION 8 SET FORTH RWS'S SOLE AND EXCLUSIVE OBLIGATIONS, AND CLIENT'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF ANY KIND.

Article 9. Support Services

9.1 ***Technical Support.*** RWS shall provide Client with online technical support for the Licensed Product at the Support Level corresponding to the Support package purchased under such Order Form. Support Services shall commence on the effective date of the applicable Order Form and shall be governed by the RWS Technical Support Service Policy (the **"Support Policy"**), available at https://rws.com/support/technical-support-service-policy/, which is incorporated into this Agreement by reference. RWS may modify the Support Policy from time to time; provided,

that any such modification shall not materially reduce the level or quality of Support Services provided under this Agreement.

Article 10. Ownership

10.1 The Licensed Product contains and/or embodies patents, copyrighted material, trade secrets, inventions and other intellectual property of RWS. RWS or its licensors retain all ownership and Intellectual Property Rights to the Licensed Product and Documentation. Client retains ownership and Intellectual Property Rights in and to the Content.

Article 11. Confidentiality

11.1 ***Exclusions.*** Confidential Information does not include information that: (i) was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party; (iii) is already in the possession of the receiving party at the time of disclosure by the disclosing party as shown by the receiving party's files and records immediately prior to the time of disclosure; (iv) is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality; or (v) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession.

11.2. ***Disclosure Restrictions.*** Each party will not disclose such Confidential Information to any third party except to those of its employees and subcontractors that need to know such Confidential Information for the purpose of performing this Agreement, provided that each such employee and subcontractor is subject to a written agreement that includes binding use and disclosure restrictions that are at least as protective as those set forth herein and each party will remain directly liable and responsible to the other party and its licensors for any violation by a party or its subcontractors hereunder. Each party will use all reasonable efforts to maintain the confidentiality of all such Confidential Information in its possession or control, but in no event less than the efforts that such party ordinarily uses with respect to its own proprietary information of similar nature and importance. The foregoing obligations will not restrict either party from disclosing Confidential Information of the other party: (a) pursuant to the order or requirement of a court, administrative agency, or other governmental body, provided that the party required to make such a disclosure gives reasonable notice to the other party to contest such order or requirement; and (b) on a confidential basis to its legal or financial advisors. In addition, each party may disclose the terms and conditions of this Agreement: (a) as required under applicable securities regulations; and (b) on a confidential basis to present or future providers of venture capital and/or potential private investors in or acquirers of such party.

Article 12. Data Privacy and Security

12.1 Data Privacy. If any Content contains any personal data or any PII or PHI, the Data Processing Agreement ("**DPA**") available at the following link https://www.rws.com/legal/privacy/dpa/ shall apply and the DPA will be incorporated herein by reference. The processing details (the duration, the nature, means and purpose of the processing, the types of personal data and categories of data subjects) shall be

specified by the Client in the reoevant Order Form to this Agreement which is hereby incorporated and forms part of the DPA.

12.2 Security. RWS shall maintain up-to-date, industry-standard security controls designed to protect the confidentiality, privacy, integrity, and availability of all data provided by or belonging to Client or its licensors, including the Content, and to prevent unauthorized access to the Licensed Product, in accordance with Exhibit B (**Security Policy**).

Article 13. Remedies

13.1 Client acknowledges and agrees that any copying or use of the Licensed Product other than as expressly permitted by this Agreement would result in irreparable injury to RWS for which money damages would be inadequate and, in such event, RWS shall have the right, in addition to other remedies available at law and in equity, to immediate injunctive relief to prevent any such unauthorized use. Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.

Article 14. Marketing Assistance

14.1 Unless otherwise agreed in an Order Form Client agrees as a part of this Agreement to actively participate in RWS's Customer Reference Program. Such participation includes use of Client's logo in RWS marketing materials, press releases or speaking engagements, use of Client's name in RWS's regulatory filings, and Client taking calls from prospective RWS customers to share Client's experiences with RWS's offering.

Article 15. Force Majeure

15.1 Neither of the parties shall be obliged to meet any obligations, including any guaranteed obligation agreed between the parties, if it is prevented from doing so as a result of force majeure. Force majeure shall include but not limited to: (i) government measures, (ii) electricity failure, (iii) faults affecting the internet, computer network or telecommunication facilities, (iv) war, (v) terrorism, (vi) riot, and (vii) acts of God. If a situation of force majeure lasts for longer than forty-five days, either of the parties shall be entitled to terminate the agreement in writing.

Article 16. Miscellaneous

16.1 ***Entire Agreement.*** This Agreement, including any Exhibits or schedules hereto, constitutes the entire and exclusive understanding and agreement between Client and RWS with respect to the subject matter hereof and supersedes all prior and/or contemporaneous agreements and understandings, written or oral, between Client and RWS with respect to the subject matter hereof. Any terms and conditions contained in any purchase order that are inconsistent with or in addition to the terms and conditions of this Agreement will be deemed stricken from such purchase order, unless expressly agreed to in writing by RWS.

16.2 ***Governing Law.*** This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation, shall be governed by and construed in accordance with the applicable Governing Law as defined in the Table 1 below, without regard to any conflict of laws principles. Except as otherwise provided in this Agreement, including Section 16.2, any legal

action or proceeding arising under it shall be brought exclusively in the Courts with Jurisdiction as determined under this Section 16.2 and venue of those courts.

Table 1 - Governing Law

Region	RWS Contracting Entity	Governing Law	Courts with jurisdiction
NASA	Propylon Inc. SDL Inc. (Mass, SDL XyEnterprise LLC	The laws of the Commonwealth of Massachusetts, United States	The courts of the Commonwealth of Massachusetts and its superior courts
	RWS Moravia India Private Limited	The laws of India	The courts of India
	RWS Translations Limited	The laws of England and Wales	The courts of England and Wales.
EMEA	SDL Limited SDL Limited RWS Translations Limited (UK)	The laws of England and Wales	The courts of England and Wales.
	SDL XyEnterprise LLC	The laws of the Commonwealth of Massachusetts, United States	The courts of the Commonwealth of Massachusetts and its superior courts
	Propylon Limited	The laws of Ireland	The courts of Ireland
	RWS Moravia India Private Limited (India)	The laws of India	The courts of India
APAC	SDL China	The laws of China	The courts of China
	SDL Singapore	The laws of Singapore	The courts of Singapore
	RWS Moravia India Private Limited (India)	The laws of India	The courts of India
	SDL XyEnterprise LLC	The laws of the Commonwealth of Massachusetts, United States	The courts of the Commonwealth of Massachusetts and its superior courts
	RWS Beijing	The laws of China	The courts of China
	KK RWS Group, Japan	The laws of Japan	The courts of Japan

16.3 ***Severability.*** If for any reason a court of competent jurisdiction finds any provision of this Agreement invalid or unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible and the other provisions of this Agreement will remain in full force and effect.

16.4 ***Amendments.*** Except as expressly agreed to by each party's authorized representative in the relevant Order Form, this Agreement may not be amended, modified, or supplemented by the

parties in any manner, except by a written instrument signed by an authorized representative of RWS and Client.

16.5 ***Waiver.*** The failure by either party to enforce any provision of this Agreement will not constitute a waiver of future enforcement of that or any other provision.

16.6 ***Assignment.*** Client will have no right to assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without RWS's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement will bind and inure to the benefit of each party's successors and permitted assigns.

16.7 ***Notices.*** All notices required or permitted under this Agreement will be in writing and delivered by confirmed facsimile transmission, by courier or overnight delivery services, or by certified mail, and in each instance will be deemed given upon receipt (notices for any applicable term renewals may also be provided via email to the address listed in the applicable Order Form). All communications will be sent to the addresses set forth above or to such other address as may be specified by either party to the other in accordance with this Section. Either party may change its address for notices under this Agreement by giving written notice to the other party by the means specified in this Section.

16.8 ***Counterparts.*** The exchange of a fully executed Agreement (in counterparts or otherwise) by digital signature or by other electronic means, such as portable document format (.pdf) file, shall be sufficient to bind the parties to the terms and conditions of this Agreement.

16.9 ***Third Party Beneficiaries.*** Except where expressly provided to the contrary, this Agreement is not intended to be for the benefit of, and shall not be enforceable by any person who, is not named at the date of this Agreement as a party to it or any person who claims rights under the Contracts (Rights of Third Parties) Act 1999 or otherwise, and neither party can declare itself a trustee for the benefit of a third party.

16.10 ***Relationship to the Parties.*** The parties to this Agreement are independent contractors and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties. Neither party will have the power to bind the other or incur obligations on the other's behalf without the other's prior written consent.

Exhibit A

Acceptable Use Policy

(for Cloud Based Licensed Products)

1.1 This Acceptable Use Policy ("AUP") governs the Client's use of the Licensed Product offered by RWS and its Affiliates. The Client may not use, or facilitate or allow others to use, the Licensed Product:

(a) for any illegal activity, including without limitation, gambling, piracy, violating copyright, trademark or other intellectual property laws;
(b) for fraudulent activity;
(c) to violate the rights of others, including invading anyone's privacy by attempting to harvest, collect, store, or publish private or personally identifiable information, such as passwords, account information, credit card numbers, addresses, or other contact information without their knowledge and consent;
(d) to access or authorize anyone to access the Licensed Product from an embargoed country;
(e) to threaten, stalk, defame, defraud, degrade, victimize or intimidate anyone for any reason, including inciting or actively encouraging violence, terrorism or other serious harm;
(f) for any content or activity that promotes child abuse, child pornography or sexual exploitation; or intending to harm or exploit minors in any way, or collecting personally identifiable information of any minor;
(g) to violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device;
(h) to use the Licensed Product to try to gain unauthorized access to any other service, data, account or network by any means;
(i) for use any automated process or service to access or use the Services such as a BOT, a spider or periodic caching of information stored by RWS;
(j) to transmit, distribute, publish, send, deliver or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations (or "spam");
(k) to falsify any email header information or in any way misrepresent the Client's identity, including misrepresenting the source of anything the Client posts or uploads or impersonating another individual or entity, such as with "spoofing";
(l) to remove, modify, or tamper with any regulatory or legal notice or link that is incorporated into the Licensed Product, including providing or creating links to external sites that violate this AUP;
(m) for any attempt to gain unauthorized access to the Licensed Product, acting to deny others access to the Licensed Product, or authorizing any third party to access or use the Licensed Product on Client's behalf (such as anyone without a license or revealing to anyone the Client's username and password); or
(n) to transmit malicious code, such as viruses, worms, time bombs, Trojan horses, and other harmful or malicious files, scripts, agents, or programs.

1.2 Client may not run on RWS's servers any program that makes the Licensed Product available to others. Client may not run such programs on their own machines connected to the RWS network in order to make such Licensed Product or resources available to others. For the avoidance of doubt, RWS expressly confirms that Client is allowed to make their own content available to others, as long as that content is compliant with this AUP.

1.3 The Client is responsible for notifying RWS immediately if Client becomes aware of an impending event that may negatively affect the Licensed Product.

1.4 The Client acknowledges that (i) neither RWS nor its suppliers or licensors exercise any control over the Client Content provided by Client when using the Licensed Product, and that it is the sole responsibility of the Client that such information complies with this AUP; and (ii) it is responsible for protecting its computers against interference, spyware or viruses that may be encountered for downloaded items from the Licensed Product.

1.5 **Investigation and Enforcement**

1.5.1 RWS may investigate any suspected violation of this AUP and may remove or disable access to any Client Content or resources that violate this AUP. The Client shall cooperate with Company to promptly remedy any such violation.

1.5.2 In determining whether a violation has occurred, RWS may consider Client's ability and willingness to comply with this AUP, including any policies and procedures Client has in place to prevent, detect, and remove prohibited content or activities.

1.5.3 Where reasonably practicable, RWS will provide prior notice to Client of any suspension under this AUP and will promptly restore the affected Licensed Product or access once the violation is resolved.

1.5.4 Violation of this AUP may result in suspension or termination of Client's account. Failure by RWS to enforce this AUP in any instance shall not constitute a waiver of its rights.

Exhibit B
Security Policy

This Security Policy outlines the minimum security and data privacy obligations that RWS shall meet when Processing Customer Content, including Personal Data (together, "**Customer Data**"), in connection with the provision of the Licensed Product under the Main Agreement. These obligations are in addition to, and do not limit, any other obligations set forth in the Main Agreement.

All capitalised terms not defined in this Security Policy shall have the meanings ascribed to them in the Main Agreement or the applicable Data Processing Agreement ("**DPA**").

LIABILITY

RWS expressly accepts responsibility for ensuring that the obligations set out in this Security Policy are fulfilled when Processing Customer Data, whether directly or indirectly through its Sub-Processors and/or third-party contractors (collectively referred to as "RWS" for the purposes of this Security Policy).

BINDING POLICIES AND PROCEDURES

RWS shall maintain documented and binding security and privacy policies and procedures ("**Security Documentation**") that comply with applicable Data Protection Laws and incorporate the requirements set out in this Security Policy. RWS shall ensure that such documentation is regularly reviewed and kept up to date.

The Security Documentation shall clearly define the physical, technical, and organisational measures implemented by RWS to protect Customer Data against unauthorised access, acquisition, use, disclosure, or destruction. Upon request, RWS shall provide the Customer with evidence that the Security Documentation is in place and current.

INFORMATION SECURITY PROGRAM

RWS shall implement and maintain an information security program, supported by a suite of policies and an organisational structure aligned with industry best practices. The program shall define clear roles and responsibilities and include the appointment of an Executive Sponsor responsible for overseeing its implementation and ongoing maintenance. The Executive Sponsor shall have the authority to allocate resources and make decisions necessary to ensure the security of Customer Data processed under this Agreement and shall report directly to RWS senior management. RWS shall regularly review and update the information security program to address emerging threats, vulnerabilities, and applicable regulatory requirements.

RISK MANAGEMENT

RWS shall conduct periodic, independent security risk assessments to identify the criticality of information assets, assess threats, evaluate potential risks, and implement appropriate risk treatment plans. RWS shall apply technical and organisational measures to mitigate identified risks, ensuring a level of security appropriate to the nature and severity of the risk.

INVENTORY

RWS shall maintain an inventory of media, servers, and equipment containing Customer Data to ensure traceability and accountability. This inventory shall include records of the return or secure destruction of Personal Data in accordance with applicable data retention and disposal policies.

PERSONNEL

RWS shall require all personnel to sign a non-disclosure or confidentiality agreement that outlines their responsibilities for protecting Customer Data and the consequences of non-compliance. RWS shall provide annual training and awareness programs on information security and data protection to all personnel, ensuring they understand their obligations and are equipped to handle Customer Data securely.

USER AUTHENTICATION

Access to RWS systems shall be strictly conditional upon the proper implementation and adherence to authentication procedures, in accordance with an approved Identity and Access Management (IAM) policy. Each user shall be assigned a unique login account, and authentication shall be enforced through secure mechanisms to prevent unauthorised access.

ACCESS MANAGEMENT

RWS shall enforce password policies that comply with applicable regulatory requirements, industry standards, and recognised best practices. Passwords shall be changed at least every 180 days, must not be reused, disclosed to others, or written down. Users shall be required to change any password assigned automatically or by an administrator. Systems shall enforce account lockout mechanisms to limit the number of failed login attempts and prevent unauthorised access.

ACCESS PRIVILEGES

Access privileges shall be granted based on predefined roles aligned with job responsibilities and the principle of least privilege. RWS shall ensure that access to Customer Data is restricted on a need-to-know basis. Outdated or unnecessary access rights shall be promptly revoked, and access permissions shall be reviewed at least annually. RWS shall implement separation of duties controls to ensure that personnel with privileged access do not simultaneously have access to other sensitive systems or data beyond their role requirements.

ENCRYPTION, HASHING AND SIGNING

RWS shall use recognised, secure cryptographic algorithms, libraries, and software to protect Customer Data. All secrets and cryptographic keys shall be securely stored and managed in accordance with industry best practices.

Customer Data shall be protected equally, regardless of classification, both in transit outside of RWS's network and at rest. This includes, but is not limited to:

- Use of strong encryption algorithms, such as Advanced Encryption Standard (AES), to prevent unauthorised access;

- Secure generation, storage, rotation, and destruction of encryption keys, ensuring sufficient key length and randomness to prevent brute-force attacks;
- Secure transmission of Customer Data using protocols such as Transport Layer Security (TLS);
- Encryption of Customer Data at rest using secure algorithms and key management practices;
- Compliance of encryption methodologies with applicable laws and regulations;
- Encryption of Customer Data prior to transmission to authorised external parties, with secrets (e.g., decryption keys) transmitted separately via a different communication channel to ensure confidentiality.

LOGGING

RWS shall maintain appropriate audit trails and system access logs for all Information Systems processing Customer Data. Logs shall be protected against tampering and monitored by trained security personnel to detect anomalies and support incident investigation and compliance requirements.

PHYSICAL AND ENVIRONMENTAL SECURITY

RWS shall implement physical and environmental security measures to prevent unauthorised physical access, damage, or interference to Customer Data and supporting infrastructure. These measures shall include, but are not limited to:

- Physical access controls to restrict access to authorised personnel only, including mechanisms such as locked doors, access cards, biometric systems, and security guards;
- Environmental controls to mitigate risks from fire, flooding, temperature fluctuations, and power outages, including fire suppression systems, water detection, HVAC systems, and backup power supplies;
- Asset management controls to track and manage equipment, hardware, and software that store or process Customer Data, including inventory systems, asset tagging, and regular inspections;
- Secure work areas with restricted access, surveillance, and physical safeguards to prevent unauthorised access or theft;
- Documented physical security policies and procedures aligned with industry standards, covering access control, environmental protection, asset management, and incident response;
- Monitoring and testing of physical security controls through regular inspections and audits;
- Secure destruction of sensitive materials, including the use of P-4 rated shredders (or higher) for hard copy records, and physical destruction of decommissioned hard drives and storage media;

- Physical access restrictions and monitoring at data center facilities, which may include multi-zone security, man-traps, perimeter deterrents (e.g., fencing, guarded gates), biometric access, CCTV, and secure cages;

- Protection of equipment and media used to process Customer Data from physical and environmental threats, including secure storage when not in use;
- Secure storage of hard copy records containing Customer Data in filing systems that support retrieval, amendment, and destruction in accordance with data subject rights;
- Use of locked containers or equivalent secure transport mechanisms for moving hard copy records, and secure destruction of such records when no longer required.

PATCH MANAGEMENT

RWS shall ensure that only licensed software is used in the provision of services and that such software complies with applicable security standards. RWS shall maintain a documented patch management process and schedule covering all infrastructure, systems, and application components used to deliver services. This process shall include the timely deployment of updates and upgrades in accordance with industry best practices.

When a vulnerability is identified and a vendor patch is available, RWS shall obtain the patch from the relevant vendor and apply it in accordance with its current vulnerability and security patch management policies and procedures. Patches shall only be deployed after appropriate testing to confirm their stability and compatibility with RWS systems. RWS shall ensure that vulnerability patches, antivirus, and anti-malware protections are applied and kept up to date, and shall not knowingly or intentionally introduce any malicious code into RWS or Customer systems.

SECURITY INCIDENT RESPONSE

RWS shall implement and maintain an incident response framework to ensure the timely identification, management, and resolution of security incidents. This shall include:

- Procedures for identifying and reporting security incidents, supported by security monitoring tools, employee awareness training, and clearly defined communication channels;
- A process for categorising and prioritising incidents based on severity and potential impact on the confidentiality, integrity, and availability of data and systems;
- Documented response procedures, including escalation paths and the involvement of incident response teams, tailored to different types of incidents;
- Root cause analysis and post-incident reviews to prevent recurrence of similar incidents;
- Maintenance of accurate and detailed records of all security incidents, including actions taken, for audit, compliance, and reporting purposes.

RWS shall notify the Customer without undue delay, and in any event within 72 hours of becoming aware of a security incident that impacts the Customer, including any Personal Data Incident. Notification shall be sent to the Customer's designated contact email address. Security incidents include, but are not limited to, extortion threats, unauthorised access, compromised user accounts or systems used to access, process, or store Customer Data, loss or theft of physical media or hard copy records containing Customer Data, and malware infections such as viruses or ransomware.

ENDPOINT SECURITY

Customer Data shall only be stored on RWS-owned equipment and assets where necessary to fulfil a defined business purpose. RWS shall implement appropriate endpoint security measures to protect against unauthorised access to Customer Data and other sensitive information. These measures shall include, at a minimum:

- Installation and maintenance of anti-malware software on all endpoint devices, with up-to-date virus definitions;
- Automatic session lockout after a predefined period of inactivity;
- Activation of host-based firewall protection on all endpoint devices;
- Regular application of security patches and software updates to protect against known vulnerabilities;
- Full-disk encryption on all endpoint devices to protect data in the event of loss or theft;
- Access controls to ensure only authorised personnel can access endpoint devices and any Customer Data stored on them;
- Regular backups and data synchronisation to ensure data availability and integrity;
- Ongoing employee training on endpoint security best practices, including adherence to RWS's security policies, phishing awareness, malware identification, and incident reporting procedures.

REMOVABLE MEDIA

RWS shall not use removable media (including USB drives, external hard drives, flash drives, CDs, DVDs, tapes, or other portable storage devices) to store Customer Data under any circumstances.

Regardless of media type, RWS shall ensure that Customer Data is protected against unauthorised access, loss, or destruction using industry-recognised security controls and in accordance with the terms of this agreement.

NETWORK SECURITY

RWS shall implement appropriate network security controls to ensure the confidentiality, integrity, and availability of systems and data. Network flows shall be restricted to what is strictly necessary, and secure remote access shall be enforced through the use of Virtual Private Networks (VPNs). Wireless networks (Wi-Fi) shall be secured using WPA3 or equivalent encryption protocols, and shall include secure identification, authentication, and encryption mechanisms. Peer-to-peer networking shall be disabled, and the use of insecure public Wi-Fi shall be prohibited.

RWS shall implement industry-standard network access controls to prevent unauthorised access to systems and data. These controls may include firewalls, intrusion detection and prevention systems (IDPS), extended detection and response (XDR), and other appropriate technologies. RWS shall regularly monitor and test network security controls to ensure they are functioning effectively.

BUSINESS CONTINUITY AND DISASTER RECOVERY

RWS shall maintain a business continuity management system aligned with ISO 22301, including a documented business continuity policy, strategy, and program. This program shall include a business continuity plan covering the Licensed Products provided by RWS, which shall be reviewed and tested periodically to ensure effectiveness.

RWS shall perform regular backups of critical systems and data, ensure that backup media is encrypted and securely stored, and implement appropriate protections during transport. Business continuity and disaster recovery procedures shall be tested regularly to ensure that Customer Data can be restored in the event of a disruption. Where RWS utilises data centers to support its services, both primary and backup data centers shall be in place. These data centers may be operated by RWS or by approved third-party providers.

ARCHIVING AND DISPOSAL

RWS shall implement appropriate access controls for archived data to ensure that only authorised personnel can access such data. Expired archives shall be securely destroyed in accordance with RWS's data retention and disposal policies.

When disposing of or repurposing equipment, physical documents, files, or media containing Customer Data, RWS shall implement appropriate measures to prevent unauthorised recovery of the data. Such measures may include secure deletion, reformatting, degaussing, or restoring devices to their original configuration.

SUB-PROCESSORS AND THIRD-PARTY PROVIDERS

RWS shall implement appropriate controls to prevent unauthorised access to Customer Data by sub-processors and third-party providers ("Third Parties"). These controls shall include:

- Conducting security risk assessments of Third Parties and approving their use based on their ability to meet RWS's security requirements for processing Customer Data;
- Regularly monitoring and auditing Third Parties to ensure ongoing compliance with applicable security requirements;
- Implementing data flow controls to ensure Customer Data is only shared with vetted and approved Third Parties;
- Requiring Third Parties to report any security incidents or data breaches involving Customer Data to RWS in a timely manner;
- Including termination rights in contracts with Third Parties in the event of non-compliance with security obligations;
- Incorporating specific data privacy and security clauses in Third Party contracts, including provisions for the return or secure destruction of Customer Data and mechanisms to verify the effectiveness of contractual safeguards (e.g., security audits or site visits).

SECURE SOFTWARE DEVELOPMENT

Where applicable, RWS shall develop secure applications for the Customer and maintain a secure software development lifecycle (SDLC) aligned with ISO/IEC 27001 standards.

Applications and websites developed and/or maintained by RWS shall be designed and tested to ensure that passwords and Personal Data are not transmitted via URL query strings or other insecure mechanisms.

RWS shall implement input validation controls to ensure that user input conforms to expected formats and does not introduce security vulnerabilities. Additionally, RWS shall implement a cookie consent banner and provide a cookie policy for any service that uses cookies, in accordance with applicable data protection laws.

RWS shall ensure logical separation between development and production environments and shall not use production or 'live' Customer Data for development or testing purposes unless the Customer has provided explicit, written consent.

RWS shall not promote software to production without first addressing all discovered vulnerabilities classified as critical or high risk, in accordance with industry-standard vulnerability scoring systems (e.g., CVSS).

SECURITY TESTING

RWS shall implement appropriate measures to discover and address vulnerabilities in RWS systems, applications and network, including but not limited:

- Conduct regular vulnerability scanning of RWSs' systems, applications and networks to identify potential security vulnerabilities, testing should be performed for OWASP Top 10+ vulnerabilities using industry recognized tools.
- Establish a patch management process to ensure that security patches and updates are promptly applied to address known vulnerabilities;
- Conduct risk assessments to identify potential vulnerabilities and prioritize their remediation based on the level of risk they pose to Customer Data;
- Conduct regular testing of RWS systems and networks to ensure that security controls are effective and to identify any new vulnerabilities;
- If applicable, ensure that third parties used by RWS for services such as cloud computing or network monitoring also address vulnerabilities in their systems and networks.
- RWS shall engage independent third parties to conduct penetration testing on its web applications to identify security vulnerabilities. These tests will be performed annually or at a minimum prior to each major release of the web application. RWS shall mitigate identified vulnerabilities according to defined security policy expectations and, upon request, provide the Customer with executive summary reports of the third-party penetration testing.

INDEPENDENT VALIDATION OF CONTROLS

RWS commits to maintaining an independent security certification, such as ISO/IEC 27001 or SOC 2 Type II, at the time of contract signature. These certifications shall be made available to the Customer for review upon request. Such certifications or attestations shall be maintained throughout the term of the contract.

RWS shall respond promptly to reasonable requests from the Customer for information about, or copies of, these certifications and attestations, including any updates or successor certifications that may apply.