Internal Workiva ID:

MAIN TERMS AND CONDITIONS

THESE MAIN TERMS AND CONDITIONS ("**Main Terms**") with any active Orders for Services and any other duly executed documents referencing these Main Terms (collectively, the "**Agreement**") shall govern Workiva's provision of Services to Customer. The Main Terms are effective on the date signed by the last party ("**Effective Date**") between Workiva Netherlands B.V. ("**Workiva**") a Dutch company with its place of business at Achtergracht 4, 1017 WP, Amsterdam, The Netherlands and, «ACCOUNT_LEGAL_NAME» ("**Customer**") a company with a business address of «ACCOUNT_CORPORATE_STREET_1» «ACCOUNT_CORPORATE_STREET_2» «ACCOUNT_CORPORATE_CITY», «ACCOUNT_CORPORATE_STATE_PROVINCE» «ACCOUNT_CORPORATE_ZIP».

1.0 Services.

1.1 Subscription Services.

(a) Workiva will provide Customer (and Customer's Affiliates as provided herein) with the Subscription Services pursuant to the terms of the Agreement. During the Subscription Term, subject to the terms of the Agreement, Workiva grants to Customer and its Users, a non-exclusive, non-transferable, worldwide right (and license only to the extent applicable to any downloadable software) to access, use, and display the Subscription Services pursuant to an applicable Subscription Order.

(b) Customer may only allow Users to access the Subscription Services on an individual user account basis. Customer is responsible for each of its Users' acts and omissions and remains liable to Workiva for any User's (including an authorized third party acting as a User on Customer's behalf) breach of the Agreement.

(c) Workiva may, in its sole discretion, update the Services; provided that such updates will be at no cost to Customer and will not materially degrade existing features and functionality. Customer is solely responsible for providing, at its own expense, all network access to the Subscription Services, including, without limitation, acquiring, installing and maintaining all telecommunications equipment, hardware, software and other equipment as may be necessary to connect to, access and use the Subscription Services. Minimum system requirements for the Subscription Services are set forth in the Documentation.

1.2 Professional Services. If applicable, Workiva will provide Professional Services as set forth in a Statement of Work.

1.3 Affiliates. Customer's Affiliate may separately purchase Services from Workiva (or a Workiva Affiliate, as the case may be), pursuant to an Order executed by such Customer Affiliate and Workiva (or Workiva Affiliate) that incorporates these Main Terms by reference ("**Affiliate Agreement**"). In such instances: (a) these Main Terms combined with any Order between Customer Affiliate and Workiva (or Workiva Affiliate) will constitute the Affiliate Agreement between Customer Affiliate and Workiva (or Workiva Affiliate), (b) Customer Affiliate shall be considered the Customer to such Affiliate Agreement, and (c) the Customer Affiliate will be solely responsible for its obligations under the Affiliate Agreement.

1.4 Usage Restrictions. Customer shall not directly or through a third party: (a) grant rights of access to the Subscription Services to anyone other than Users without Workiva's prior written consent; (b) sell, resell, assign (except as set forth in Section 10.6 - Assignment), lease, rent, sublicense, or otherwise transfer or make available the rights granted to Customer under the Agreement for use by third parties, in whole or in part, without Workiva's prior written consent; (c) reverse engineer, decompile, or disassemble any Subscription Services or otherwise attempt to discover the source code thereof; (d) attempt to disable or circumvent any security measures in place; (e) reproduce or copy the Subscription Services, in whole or in part; (f) modify, adapt, or create derivative works of the Subscription Services, in whole or in part, or permit any third party to do so; (g) delete, remove, modify, obscure, fail to reproduce, or in any way interfere with any proprietary, trade secret, or copyright notice appearing on or incorporated into the Subscription Services; (h) use Subscription Services to store or transmit libelous or otherwise unlawful or tortious material or any material in violation of third party privacy rights; (i) interfere with or disrupt the integrity or performance of Subscription Services or third party data contained therein; or (j) use or attempt to use any portion of the Subscription Services in a manner that is unauthorized or would exceed the scope granted under the Agreement, or facilitate any such unauthorized access or use for any third party. If any unauthorized access or use occurs, Customer shall: (a) promptly notify Workiva of the incident, and (b) reasonably cooperate in resolving the issue.

2.0 Security; Customer Data.

2.1 Security and Data Privacy. Workiva shall maintain appropriate administrative, physical, and technical safeguards to protect the security, confidentiality and integrity of Customer Data, as described in Workiva's security standards set forth in Exhibit A ("**Security Standards**"). To the extent Customer Data includes Customer Personal Data (as defined in the DPA), Workiva will only process such data pursuant to Customer's requests or as otherwise set forth in Exhibit B ("**Data Processing Agreement**" or "**DPA**").

2.2 Customer Data; Responsibilities. Except as otherwise provided in the Agreement (or instructed by Customer), Workiva shall only process Customer Data to provide the Services and enforce its rights under this Agreement. Workiva will neither have the responsibility to review, nor any liability as to the accuracy or integrity of, any information or content posted by Customer or its Users.

2.3 Usage Data. Notwithstanding anything contrary in this Agreement, Workiva may collect, store and use data (excluding Customer Data) relating to or derived from the operation or Customer's or Users' use of the Services ("**Usage Data**"). Workiva may use Usage Data for diagnostic and corrective purposes, to improve and develop the Services and Workiva's other offerings, and to operate Workiva's business. To the extent Usage Data contains any Personal Data, Workiva is the Controller of such Personal Data and will process such Personal Data in accordance with Applicable Data Protection Law (as these terms are respectively defined in the DPA) and Workiva's Services Privacy Policy (available here: https://www.workiva.com/legal/services-privacy-policy). Subject to Section 5.0 (Confidentiality), Workiva may share Usage Data with third parties only if it is aggregated and anonymized such that Customer and its Users cannot be identified. Workiva will be the owner of any intellectual property generated through Workiva's use of Usage Data.

3.0 Fees; Payment.

3.1 Invoicing and Renewals. Fees are payable in advance or in accordance with any billing frequency or terms stated in the Order. Unless otherwise specified in the applicable Order, Customer shall pay all undisputed Fees no later than thirty (30) days from date of invoice ("**Payment Period**"). If undisputed Fees are not paid in full fifteen (15) days after the invoice due date ("**Grace Period**"), Workiva has the right to suspend all Services provided under the Agreement until Customer pays in full. Workiva will provide a ten (10) day prior notice of pending suspension. If Customer requires the use of a third party for invoice processing, Customer shall be the sole bearer of any cost and expense associated with such third party. Any written notice of an Order renewal shall include the applicable Fees for such renewal period and be provided to Customer at least forty-five (45) days prior to the expiration thereof.

3.2 Disputes. If Customer disputes an invoice in good faith, Customer will notify Workiva within the Payment Period and the parties will seek to resolve the dispute. Customer is not required to pay disputed Fees prior to resolution, but will timely pay all undisputed Fees. Upon resolution, if applicable, Customer will pay such Fees found to be due and owing as soon as reasonably practicable.

3.3 Use Verification. Workiva may review use of the Services in order to verify Customer's compliance with the scope and terms of this Agreement and/or any Subscription Order. If Workiva determines that Customer is exceeding its permitted access and usage rights granted under this Agreement or a Subscription Order, Workiva will provide written notice per Section 10.4 (Notice) to Customer regarding such potential or actual non-compliance. If Customer fails to then (i) cure its non-compliance within thirty (30) days of such notice or (ii) to provide Workiva with temporary remote access to its environment for the limited purpose of verifying compliance, Workiva may, at its sole discretion, (a) suspend Customer's Services, or (b) terminate the applicable Order(s). If necessary to resolve any continuing non-compliance, Workiva may request that Customer enter into an Order to purchase additional Subscription Services as necessary to reflect Customer's actual usage. Any such Order shall be mutually agreed upon and executed by both parties.

3.4 Taxes. Fees stated in the Orders do not include applicable taxes. Except for taxes based on Workiva's net income or property, Customer shall be responsible for payment of all applicable taxes, impositions, fees, or other charges that arise in any jurisdiction as a result of the Services provided under the Agreement, including without limitation all sales, use, value added, consumption, gross receipts (other than in lieu of net income tax), excise, stamp or transfer taxes, however designated. Customer shall pay any such tax when due or reimburse Workiva at Workiva's request. If Customer is exempt from such taxes, Customer shall provide Workiva with a certificate or permit documenting this exemption. If Customer is required to withhold or deduct any portion of the Fees, then Workiva shall be entitled to receive from Customer such amounts as will ensure that the net receipt, after tax and duties, to Workiva in respect of the Fees is the same as it would have been were the payment not subject to the tax or duties. If Workiva is required to pay any taxes on behalf of Customer due to a change in facts, circumstances, or tax legislation, the full amount of such tax will be billed to Customer separately, whether or not during the Agreement Term, and promptly paid by Customer as further

limited by any applicable statute of limitations. Workiva and Customer agree to cooperate to reduce any tax liability related to this Agreement.

3.5 Purchase Orders. Customer acknowledges that providing a purchase order is solely for Customer's administrative convenience and does not discharge Customer's obligations under an applicable executed Order. For the avoidance of doubt, invoices and/or the Fees therein may not be disputed for Customer's failure to provide administrative information, including purchase order numbers, contract numbers or IDs, or any other administrative information of a similar nature.

4.0 Term; Termination.

4.1 Agreement Term. The Agreement begins on the Effective Date, and continues until all Orders associated with the Agreement have expired or been terminated (the "**Agreement Term**").

4.2 Subscription Term. The Subscription Services will begin on the Start Date defined in a Subscription Order and remain in effect for the period specified therein (the "**Subscription Term**"). The parties may agree to renew the Subscription Services as set forth in the applicable Subscription Order which will control in cases of conflict with this Section.

4.3 Statements of Work Term. The period of performance for Professional Services will be set forth in the applicable SOW.

4.4 Termination without Cause. Customer may terminate the Agreement or any individual Order without cause upon thirty (30) days written notice. If Customer terminates a Subscription Order without cause, Customer will remain responsible for all Subscription Services Fees. If Customer terminates a Statement of Work without cause, Workiva will refund any prepaid but unearned Professional Services Fees outstanding as of the effective date of such termination. If Customer exercises its rights under this Section, any unpaid Fees shall be payable by Customer on or prior to the effective date of such termination, even if such Fees are related to unused access to the Subscription Services.

4.5 Termination for Cause. Either party may terminate the Agreement, or any individual Order, for a material breach by the other party that is not cured within thirty (30) days after written notice of such material breach. If the Agreement is terminated due to Workiva's uncured material breach, within thirty (30) days of the termination effective date Workiva will refund a pro-rated portion of Fees for the remainder of the Agreement Term.

4.6 Termination for Bankruptcy. Either party may terminate the Agreement or any individual Order if the other party becomes insolvent, bankrupt, or ceases to do business.

5.0 Confidentiality.

5.1 Confidential Information. Each party may disclose (the "**Disclosing Party**") to the other (the "**Receiving Party**") Confidential Information during the course of the Agreement. Except as otherwise agreed upon in writing, each party agrees that Confidential Information includes: (a) all information communicated by the Disclosing Party in connection with the Agreement and identified as confidential, (b) any information exchanged between the parties in connection with Customer's purchase of any additional Services (including information related to future business relationships or Services not currently addressed under the Agreement, such as requests for proposals, bids, correspondence, negotiations, and other discussions), (c) the terms of the Agreement, and (d) all information communicated by a Disclosing Party that a reasonable person would understand to be confidential to the Disclosing Party. Workiva Confidential Information includes the Services, Fees, Workiva's development plans, any security specifications, and reports or assessments related to the Services, Workiva or its licensors and third parties. Customer Confidential Information includes Customer Data.

5.2 Standard of Care; Third Parties. Receiving Party will use at least the same degree of care to safeguard the Confidential Information of the Disclosing Party as it employs for its own information (or information of its customers) of a similar nature, and in any event, no less than reasonable care. Receiving Party will limit access to Disclosing Party's Confidential Information to its employees, consultants, contractors, advisors and other third parties ("**Representatives**") subject to written confidentiality obligations at least as restrictive as those set forth in the Agreement (or other professional or fiduciary obligations of confidentiality), and have a need to know. Receiving Party will be responsible for any improper disclosure or use of Confidential Information by its Representatives.

5.3 Restrictions. Receiving Party will not (a) use Confidential Information of Disclosing Party except to fulfill its rights and obligations under the Agreement, (b) acquire any right in or assert any lien against the Confidential Information of Disclosing Party, or

(c) sell, assign, lease, or otherwise commercially exploit the Confidential Information (or any derivative works thereof) of Disclosing Party. The Receiving Party may not withhold or refuse for any reason (including due to the other Disclosing Party's actual or alleged breach of the Agreement) to promptly return to the Confidential Information of the Disclosing Party (including copies thereof) if requested to do so.

5.4 Return and Destruction. Upon expiration or termination of the Agreement and completion of Receiving Party's obligations under the Agreement, Receiving Party will, as requested by Disclosing Party, return or destroy Disclosing Party's Confidential Information. Workiva will fulfill the obligation to return Customer Data by providing one (1) User with access to the Subscription Services, for a period not to exceed thirty (30) days, solely to allow such User to download Customer Data in the file formats set forth in the Documentation. For clarity, provision of User access as described in the previous sentence enables Customer to directly access, delete, download, or transition its Customer Data out of Workiva's platform without Workiva accessing, downloading, storing, or transmitting Customer Data. If additional termination-related data retrieval or transition services are requested by Customer, any such services will be subject to a mutually executed SOW. Subject to the foregoing confidentiality obligations, either party may retain copies of the Confidential Information of the other party to the extent required to document its performance or for compliance with applicable laws or regulations.

5.5 Exclusions; Permitted Use. This Section 5.0 will not apply to any information that Receiving Party can demonstrate: (a) was, at the time of disclosure, in the public domain, (b) after disclosure, is published or otherwise becomes part of the public domain through no fault of the Receiving Party, (c) was, at the time of disclosure, in the possession of Receiving Party and was not the subject of a pre-existing confidentiality obligation, (d) was received after disclosure from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations), or (e) was independently developed by or for Receiving Party without use of the Confidential Information of Disclosing Party. In addition, Receiving Party will not be in breach of this Section 5.0 for disclosing Confidential Information of Disclosing Party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request, to the extent legally permissible, Receiving Party advises Disclosing Party prior to making such disclosure and provides a reasonable opportunity to Disclosing Party to object to such disclosure, take action to ensure confidential treatment of the Confidential Information, or (subject to applicable law) take such other action as it considers appropriate to protect the Confidential Information.

5.6 Unauthorized Access. Receiving Party will: (a) notify Disclosing Party promptly of any material unauthorized possession, use, disclosure, or knowledge of Disclosing Party's Confidential Information that becomes known to Receiving Party, (b) promptly furnish to Disclosing Party details of the unauthorized possession, use, disclosure, or knowledge, or attempt thereof, and use reasonable efforts to assist Disclosing Party in investigating or preventing the recurrence of any unauthorized possession, use, or knowledge, or attempt thereof, of Confidential Information, (c) use reasonable efforts to cooperate with Disclosing Party in any litigation and investigation against third parties deemed necessary by Disclosing Party to protect its proprietary rights, and (d) promptly use reasonable efforts to prevent a recurrence of any such unauthorized possession, use, or knowledge of Confidential Information.

6.0 Ownership; Feedback; RPA.

6.1 Workiva Ownership. Workiva (or its licensors) retains all ownership of, and title to, all intellectual property rights in, the Services, and all software, equipment, processes, facilities, and materials utilized by or on behalf of Workiva to provide the same, including all patents, trademarks, copyrights, trade secrets, and other property or intellectual property rights. Customer acknowledges and agrees Workiva (or its licensors) shall own all right, title and interest in and to any modifications, derivative works, expansions or improvements to the Services, without any other or subordinate right whatsoever being held by Customer. Customer shall acquire no rights other than those limited rights of use specifically conferred by this Agreement. All rights related to the Services that are not expressly granted to Customer under the Agreement are reserved by Workiva (or its licensors).

6.2 Customer Ownership. As between Workiva and Customer, Customer is the owner of all Customer Data. Workiva will only process Customer Data to provide the Services and in accordance with the Agreement or as otherwise permitted by Customer in writing.Workiva acquires no right, title, or interest from Customer or its Users to Customer Data, including any intellectual property rights therein. Customer will own any reports or documents generated through Customer's use of the Subscription Services in accordance with this Agreement. If such reports or documents include any pre-existing intellectual property owned by Workiva, Workiva hereby grants to Customer a worldwide, perpetual, nonexclusive, royalty-free, and irrevocable license to copy, modify, create derivative works of and distribute, license and sublicense such pre-existing intellectual property to the extent made a part of Customer's reports or documents.

6.3 Feedback. “**Feedback**” means comments, suggestions, or other feedback provided by Customer or its Users regarding the Services, or Preview Feature(s). If Customer or its Users provide Workiva with Feedback, Customer hereby grants Workiva a perpetual, irrevocable, royalty-free, fully paid-up, worldwide license to use such Feedback. Workiva has the right, but not the obligation, to use such Feedback in any way without restriction or obligation to Customer. Workiva will be the exclusive owner of any modifications, enhancements, or derivative works of the Services resulting from Workiva’s use of such Feedback. Feedback excludes Customer Confidential Information.

6.4 RPA. Customer may use and deploy RPAs when accessing the Subscription Services, subject to the terms of this Section 6.4. Workiva may immediately suspend such RPAs (or the Services as a whole, if reasonably necessary), if the RPAs (i) disrupt the integrity or performance of the Services or any data of Workiva’s other customers, or (ii) infringe, or allegedly infringe, the intellectual property rights of a third party. Workiva will provide Customer with subsequent notice regarding any such suspension. If Workiva is unable to suspend such RPAs in accordance with the foregoing, Customer agrees to immediately, upon Workiva’s request, discontinue use of, and/or suspend such RPAs. Customer is solely responsible for RPAs.

7.0 Warranties; Disclaimers; Compliance with Laws.

7.1 Mutual Representations and Warranties. Each party represents and warrants that: (a) it possesses the full right, power, and authority to enter into the Agreement and perform its obligations hereunder, (b) the execution of the Agreement by its representative(s) has been duly authorized by all necessary corporate or organizational action of such party, and (c) when executed and delivered by both parties, an Order incorporating these Main Terms will constitute the legal, valid, and binding obligation of such party, enforceable in accordance with its terms.

7.2 Workiva Representations and Warranties. Workiva represents and warrants: (a) that the Subscription Services will perform materially in accordance with the Documentation and the Agreement, (b) to use commercially reasonable efforts to correct material defects that are reported by Customer or its Users, (c) to perform the Services in a timely, professional, and workmanlike manner with a level of care, skill, practice, and judgment consistent with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience, and qualifications, and will devote adequate resources to meet Workiva’s obligations under the Agreement, (d) it will update the Documentation so that it continues to describe the Subscription Services and Services in all material respects, and (e) the Subscription Services do not contain code intended to disrupt, damage, or interfere with Customer systems, software, or Customer Data. Customer acknowledges and agrees that in order to receive the benefit of the stated service levels in the Order, and in order to reserve rights under this Section 7.2, Customer must remain in compliance with Workiva system requirements set forth in the Documentation.

7.3 Compliance with Laws.

(a) Each party represents and warrants that it shall at all times comply with all applicable laws, regulations and good business practices when performing its duties under the Agreement.

(b) If either party takes an action that violates applicable anti-bribery, anti-corruption, or anti-slavery laws and all associated and/or successor legislation and regulation, the non-violating party may immediately terminate the Agreement in accordance with Section 4.5 (Termination for Material Breach) without further obligation or liability hereunder.

(c) Customer acknowledges that Workiva’s Subscription Services are of United States origin and thus cannot be accessed in countries or by Users that are subject to the U.S. Treasury Department’s list of Specially Designated Nationals or the U.S. Department of Commerce Denied Persons List or Entity List (in either case, a "**Sanctions List**"). Customer acknowledges that the Services may not be exported or re-exported to any countries on the Sanctions List, which are subject to change from time to time without notice and limitation. Workiva reserves the right to block Users' access if they are located in any embargoed country. In addition, Workiva may, without notice, immediately suspend a User if such a User is subject to the Sanctions Lists. Customer represents and warrants that Customer and any Customer director, officer, agent, employee, affiliate or other person associated with or acting on Customer’s behalf or any of its affiliates or subsidiaries is not included within any Sanctions List.

(d) Customer acknowledges the Services are not designed to handle data or include services subject to International Traffic in Arms Regulations and agrees not to store, transmit, or introduce any such information into the Services.

7.4 Customer Acknowledgments. As between the parties, Customer is solely responsible for obtaining all necessary rights and consents to enter Customer Data into the Subscription Services. Customer hereby represents and warrants that (a) Customer has sufficient rights to provide Customer Data to Workiva under the Agreement, and (b) Customer Data will not violate or infringe the rights of any third party. Customer further acknowledges that neither Workiva nor the Subscription Services is a primary system of record of Customer Data, and Customer shall regularly backup any files for which it intends as such. Subject to 7.2(b), if a malfunction in the Services is due to a problem with Customer hardware or software, Workiva will inform Customer and it will be Customer's responsibility to obtain and pay for any required repairs or modifications.

7.5 Disclaimers.

(a) EXCEPT AS SPECIFICALLY SET FORTH IN THE AGREEMENT, AND TO THE FULLEST EXTENT PERMITTED BY LAW, (I) THE SERVICES ARE PROVIDED ON AN "AS IS" BASIS AND WORKIVA DOES NOT REPRESENT OR WARRANT THAT THE SERVICES (A) WILL BE UNINTERRUPTED OR ERROR FREE, OR (B) WILL OPERATE IN COMBINATION WITH OTHER HARDWARE OR SOFTWARE UNLESS SUCH HARDWARE OR SOFTWARE IS THIRD PARTY SOFTWARE OR HARDWARE OR SOFTWARE EXPRESSLY APPROVED OR RECOMMENDED BY WORKIVA; AND (II) WORKIVA, ITS LICENSORS, AND SERVICE PROVIDERS DO NOT MAKE, AND EXPRESSLY DISCLAIM, ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE.

(b) Customer acknowledges and agrees that Workiva and its licensors are not responsible for: (i) the performance of Customer's or its Users' equipment, hardware, RPA, software, network, and internet connection; or (ii) delays, delivery failures, or other loss or damage resulting from the transfer of data over communications networks and facilities which are not owned by Workiva or under its direct control, including Customer's or its Users' connection to the internet, and Customer acknowledges that the Subscription Services may be subject to limitations, delays, and other problems inherent in the use of such communications facilities.

8.0 Infringement Indemnification.

8.1 Workiva Indemnification. Workiva will: (a) defend Customer from and against any claim by a third party alleging that the Subscription Services, when used as authorized under the Agreement, infringes such third party's patents, copyrights, or trademarks, and (b) in relation to such claim, indemnify and hold harmless Customer from any actual and reasonable costs and expenses incurred in cooperating with Workiva's defense of the claim and from any damages and costs awarded by a court or agreed to in settlement by Workiva (including reasonable attorneys' fees).

8.2 Customer Indemnification. Customer will (a) defend Workiva from and against a claim by a third party alleging Customer Data infringes such third party's patents, copyrights, or trademarks, and (b) in relation to such claim, indemnify and hold harmless Workiva from any actual or reasonable costs and expenses incurred in cooperating with Customer's defense of the claim and from any damages and costs awarded by a court or agreed to in settlement by Customer (including reasonable attorneys' fees).

8.3 Procedures for Indemnification. The obligations of the party required to indemnify pursuant to Sections 8.1 or 8.2 ("**Indemnitor**") are expressly conditioned on the party being indemnified ("**Indemnitee**"), (a) promptly notifying Indemnitor in writing of any such claim of which Indemnitee has actual knowledge (provided that failure to do so will only release Indemnitor from this obligation to the extent that such failure led to material prejudice), (b) granting Indemnitor sole control of the defense of any such claim and of all negotiations for its settlement or compromise in writing, provided that no such settlement or compromise may impose any monetary or other obligations on Indemnitee, and (c) reasonably cooperating with Indemnitor to facilitate the settlement or defense of the claim.

8.4 Replacement. Should the Subscription Services become, or if in Workiva's opinion are likely to become, the subject of a claim of infringement of a patent, trade secret, trademark, or copyright, Workiva may (a) procure for Customer, at no additional cost to Customer, the right to continue to use the Subscription Services, (b) replace or modify the Subscription Services, at no cost to Customer, to make it non-infringing, provided that the same material function is performed by the replacement or modified Subscription Services, or (c) if in Workiva's judgment the aforementioned "(i)" and "(ii)" are not commercially feasible, terminate the Agreement (or the applicable Order) and grant Customer a pro-rated refund of any advance Fees paid applicable to the remainder of the Subscription Term.

8.5 Combination. Workiva shall have no obligation under the foregoing with respect to any claim arising from: (a) the combination or use of the Subscription Services with any technology, software, hardware or services not provided by Workiva where the infringement would not have occurred but for such combination or use, unless there is no commercially reasonable non-infringing use of the Subscription Services without such use or combination, (b) Customer's non-compliance with Section 1.4 (Usage Restrictions), or (c) Customer's modification of the Subscription Services.

8.6 Limitation. This Section 8.0 states the entire liability of Indemnitor with respect to third party infringement arising from the Services, Software, or Customer Data, or any parts thereof, and Indemnitor shall have no additional liability with respect to any alleged or proven infringement.

9.0 **Disclaimer of Certain Damages and Limitation of Liability**.

9.1 DISCLAIMER OF CERTAIN DAMAGES. EXCEPT AS SET FORTH IN THIS SECTION 9.0, TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES IN CONNECTION WITH THE SERVICES, OR THE PERFORMANCE OR NONPERFORMANCE OF SERVICES OR ANY ORDER, REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.2 LIMITATION OF LIABILITY. EACH PARTY'S AGGREGATE LIABILITY UNDER THE AGREEMENT SHALL BE LIMITED TO THE ACTUAL AMOUNT PAID OR PAYABLE BY CUSTOMER DURING THE TWELVE (12) MONTHS PRIOR TO SUCH CLAIM(S) FOR THE SPECIFIC SERVICE(S) GIVING RISE TO SUCH CLAIM(S), PROVIDED WORKIVA'S LIABILITY FOR ITS BREACH OF ITS OBLIGATIONS UNDER SECTION 5.0 (CONFIDENTIALITY), EXHIBIT A (SECURITY STANDARDS), AND EXHIBIT B (DPA) SHALL BE LIMITED TO AN AMOUNT EQUAL TO TWO TIMES (2X) THE ACTUAL AMOUNT PAID OR PAYABLE BY CUSTOMER DURING THE TWELVE (12) MONTHS PRIOR TO SUCH CLAIM(S) FOR THE SPECIFIC SERVICE(S) GIVING RISE TO SUCH CLAIM(S).

9.3 Exclusions to the Limitation on Liability. The limitations in Sections 9.1 and 9.2 shall not apply to: (a) either party's indemnity obligations set forth in Section 8.0, (b) either party's gross negligence, fraud, criminal acts or willful misconduct, (c) Customer's payment obligations.

10.0 Miscellaneous.

10.1 Public Announcements. Unless otherwise agreed by Customer in writing, Customer hereby grants Workiva the right to use Customer's name and/or logo in Workiva's marketing materials, social media and websites.

10.2 Preview Features. Workiva may, at its discretion, invite Customer to access and use Preview Features. Preview Features will be further described on Workiva's website, which will be made available to Customer at the time of the invitation. Customer is under no obligation to accept Workiva's Preview Feature invitation. Customer will have access to the Preview Feature for the period of time specified in the invitation. Preview Features are not part of the Subscription Services provided by Workiva pursuant to these Main Terms; provided that Customer's use of Preview Features is free of charge and for technical evaluation only, and any other restrictions in the Agreement that apply to the Subscription Services shall also apply to the Preview Feature. Customer's use of a Preview Feature is subject to the Preview Feature Terms.

10.3 Relationship of the Parties. The parties agree they are independent parties. Neither party shall be considered to be a partner, joint venture, employer, or employee of the other under the Agreement. The Agreement creates no agency in either party, and neither party has any authority whatsoever to bind the other party in any transaction or make any representations on behalf of the other party.

10.4 Notice. Any notice or demand which is required to be given under the Agreement will be deemed to have been sufficiently given and received for all purposes when delivered by: (a) hand, (b) confirmed electronic transmission, (c) nationally recognized overnight courier, or (d) five (5) days after being sent by certified or registered mail, postage and charges prepaid, to the mailing address or e-mail address identified in the applicable Order, and to the attention of such other person(s) or officer(s) as either party may designate by written notice.

10.5 Governing Law; Dispute Resolution. The Agreement and any issues, disputes, or claims arising out of or in connection with it (whether contractual or non-contractual in nature such as claims in tort, from breach of statute or regulation or otherwise) shall be governed by, and construed in accordance with, the laws of the Netherlands. Any dispute or claim arising out of or in connection with

the Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the Rules of the LCIA, which rules are deemed to be incorporated by reference into this Section. Any arbitration commenced pursuant to this Section shall be administered by the LCIA. The appointing authority shall be the LCIA. The standard LCIA Administrative Procedures and Schedule of Costs shall apply. The number of arbitrators shall be three (3). The place of arbitration shall be London, UK. The language to be used in the arbitral proceedings shall be English. Notwithstanding, either party may take proceedings or seek remedies before the courts or any competent authority of any country for interim or interlocutory remedies in relation to any infringement by the other party of its intellectual property rights.

10.6 Assignment. Neither party may assign the Agreement, or any of its interests herein, without the prior written consent of the other party, which consent may not be unreasonably withheld or delayed; provided, however, that no such prior approval shall be required for an assignment in connection with (a) a sale of all or substantially all of a party's business related to the subject matter of the Agreement, (b) any merger, sale of a controlling interest, or other change of control of such party, or (c) a party's assignment of all or part of its obligations under this Agreement to an Affiliate. In the event of assignment as mentioned in the previous sentence, the assigning party shall provide written notice as soon as is reasonably practicable. The Agreement applies to and binds the permitted successors and assigns of the parties.

10.7 Force Majeure. Neither party will be in default or otherwise liable for any delay in, or failure of, its performance under the Agreement if such delay or failure arises due to a Force Majeure Event. If either party is unable to perform, or is delayed in performing, its obligation under this Agreement due to a Force Majeure Event, the party so affected by the Force Majeure Event will promptly give notice to the other party. Both parties agree to use commercially reasonable efforts to mitigate the impact of a Force Majeure Event. If a delay or failure due to a Force Majeure Event continues for more than thirty (30) consecutive days, either party may cancel the underperformed Subscription Order or Statement of Work by immediately terminating the affected Order upon written notice. Customer shall be entitled to a refund of any pre-paid unused Fees for the terminated Order from the date of termination notice. This Section does not excuse either party's obligation to take reasonable steps to follow its normal disaster recovery procedures or Customer's obligations to pay for the Services up until date of termination.

10.8 Injunctive Relief. Each party acknowledges and agrees that a breach, including an anticipatory or threatened breach, by either party of its obligations under Sections 5.0 (Confidentiality) or 6.0 (Ownership; Feedback; RPA) may cause immediate and irreparable harm to the non-breaching party for which monetary damages may not constitute an adequate remedy. Accordingly, the non-breaching party shall be entitled to seek injunctive relief for the breaching party's obligations herein, without the non-breaching party having to prove actual damages and without the posting of bond or other security. Such remedy shall not be deemed to be the exclusive remedy for the breaching party's breach of the Agreement, but shall be in addition to all other remedies available to the non-breaching party at law or in equity.

10.9 Third Parties. Based on the particular Services being provided, certain third party pass-through terms may be required to be accepted by Customer. Such third party terms will take precedence in cases of conflict with these Main Terms. No other third party will be a beneficiary of the Agreement or be entitled to directly enforce the terms of this Agreement, unless otherwise explicitly set forth in a mutually executed Order. Workiva may subcontract provision of Services to its Affiliates and to third parties provided that it will remain responsible for breaches of the Agreement caused by such third parties.

10.10 Inside Information. The parties acknowledge certain restrictions may be imposed on Customer and Workiva if the Customer Data includes inside information within the meaning of the European market abuse regulation (the "Inside Information"). Customer assumes the task to draw up and update an insider list for Workiva if employees and service providers from Workiva have access to Inside Information. Workiva shall maintain an access log functionality as described in the Documentation and shall on Customer's request collaborate with Customer to provide the information of any Workiva employee as required by applicable law, where permissible and subject to applicable labour or privacy law. In case of a regulator's request, Customer shall provide Workiva with an up to date copy of the insider list that enables Workiva to comply with the applicable provisions under the European market abuse regulation. Workiva confirms that its employees and service providers that have unencrypted access have been informed as to the confidential nature of Customer's pre-release data and the importance of preserving its confidentiality, including refraining from trading in Customer's securities while in possession thereof.

10.11 Electronic Storage. Electronic imaging and storage of the Agreement is permitted. The admissibility into evidence of such an image instead of the original paper version of the Agreement is valid, if signed by both parties. The parties stipulate that any computer printout of any such image of the Agreement shall be considered to be an "original" under the applicable court or arbitral rules of evidence when maintained in the normal course of business and shall be admissible as between the parties to the same extent and under the same conditions as other business records maintained in paper or hard copy form. The parties agree not to

contest, in any proceeding involving the parties in any judicial or other forum, the admissibility, validity, or enforceability of any image of the Agreement because of the fact that such image was stored or handled in electronic form.

10.12 Survival. Expiration or termination of the Agreement will not terminate those obligations and rights of the parties pursuant to provisions of the Agreement (i.e.: Customer's outstanding payment obligations) which by their express terms are intended to survive and such provisions will survive the expiration or termination of the Agreement. Without limiting the foregoing, the respective rights and obligations of the parties under Sections 1.0 (Services), 5.0 (Confidentiality), 6.0 (Ownership; Feedback; RPA), 7.0 (Warranties; Disclaimers; Compliance with Laws), 9.0 (Disclaimer of Certain Damages and Limitation of Liability), 10.0 (Miscellaneous), and 11.0 (Definitions) of these Main Terms will survive the expiration or termination of the Agreement regardless of when such termination becomes effective.

10.13 Waiver. The waiver by either party of a breach or violation of any provision of the Agreement shall be in writing, and (unless otherwise agreed in writing) will not operate as, or be construed to be, a waiver of any subsequent breach of the same or any other provision hereof.

10.14 Enforceability. If any provision of the Agreement is held to be unenforceable for any reason, the unenforceability thereof will not affect the remainder of the Agreement, which will remain in full force and effect and enforceable in accordance with its terms. With respect to any unenforceable provision, the applicable arbitrator or court shall deem the provision modified to the extent necessary, in such adjudicator's opinion, to render such term or provision enforceable, and the rights and obligations of the parties will be construed and enforced accordingly, preserving to the fullest permissible extent the intent and agreements of the parties set forth herein. Headings in these Main Terms shall not be used to interpret or construe its provisions.

10.15 Order of Precedence. The following order of precedence will be followed in resolving any inconsistencies between the terms of these Main Terms and the terms of any Orders, exhibits, or other documents: first, Sections 1.0 – 11.0 of these Main Terms, including the attached exhibits (which may give priority to Orders for certain purposes); second, terms contained in an Order; and third, the terms of any other documents referenced in any of the foregoing.

10.16 General. On the Effective Date, the Agreement supersedes all previous discussions, negotiations, understandings, and agreements between the parties with respect to its subject matter, including any non-disclosure agreements and/or obligations which will be expressly superseded in their entirety by Section 5.0 (Confidentiality) of these Main Terms, and constitutes the entire Agreement between the parties with regard to the subject matter herein. No oral statements or material not specifically incorporated herein will be of any force and effect. The Agreement will not be construed against either party as the purported drafter. The parties shall reasonably cooperate with each other to provide such further assurances as may be reasonably required to better evidence and reflect, or to show the ability to carry out the intent, purposes, and obligations of the Agreement. With the exception of any terms or conditions that have been accepted or acknowledged (electronically or otherwise) by Customer or a User via Workiva's website or the Subscription Services, no changes in or additions to these Main Terms will be recognized unless incorporated herein by amendment, or as mutually agreed in an Order, and signed by duly authorized representatives of both parties. The application of Customer's general terms and conditions in any vendor acknowledgement or Customer's other general purchasing conditions are hereby expressly excluded and objected to by Workiva. These Main Terms shall apply and supersede the pre-printed terms and conditions of any form submitted, in electronic format or otherwise, by either party.

11.0 Definitions. The following capitalized terms used in the Agreement have the meanings set forth below:

11.1 "**Affiliate**" means any person or entity that directly or indirectly controls, is controlled by, or is under common control with either Customer or Workiva, as applicable. For purposes of this definition the term "controls", "is controlled by" or "under common control with" means the direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity, or the power to otherwise direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities, by contract or otherwise.

11.2 "**Confidential Information**" is information that relates to the Disclosing Party's business operations, financial condition, customers, products, services, or technical knowledge.

11.3 "**Customer Data**" means any data or information uploaded, inputted or edited by Customer or its Users (or by Workiva at Customer's or a User's request) into the Subscription Services, including fonts, documents, RPA and other content.

11.4 "**Documentation**" means the manuals, specifications, and other materials describing the functionality, features, and operating characteristics of the software, available at support.workiva.com, including any updates thereto.

11.5 "**Fees**" means fees for Services as set forth in an applicable Order.

11.6 "**Force Majeure Event**" means a delay or failure that arises due to any reason beyond a party's reasonable control, including pandemics, earthquakes, floods, fires, acts of civil, governmental, regulatory, or military authority, terrorism, riots, or failures or delays in transportation or communications.

11.7 "**Order**" may refer to either a Subscription Order or Statement of Work (collectively, "**Orders**").

11.8 "**Preview Feature**" means proprietary features that are not generally available to Workiva's customer base, including but not limited to any services or features referenced as "beta", "early adopter", "limited availability", "preview", or "pre-release".

11.9 "**Preview Feature Terms**" means the terms and conditions that apply to any Preview Features made available to Customer, as further set forth here: https://www.workiva.com/legal/preview_feature_terms.

11.10 "**Professional Services**" means setups, trainings, and other professional services provided by Workiva as set forth in an applicable SOW.

11.11 "**Robotic Process Automation**" or "**RPA**" refers to robotic process automation, computer scripts, or any similar type of non-human Users introduced by Customer or Customer's Users into the Subscription Services.

11.12 "**Services**" means Subscription Services and Professional Services.

11.13 "**Statement of Work**" or "**SOW**" means an ordering document for Professional Services.

11.14 "**Subscription Order**" means an ordering document for Subscription Services.

11.15 "**Subscription Services**" means subscription based access, exercisable through Customer's Users, to Workiva's cloud based software programs which are made up of Workiva's proprietary software, the Documentation, incidental downloadable software created by Workiva, support, and applicable Third Party Software, as more adequately described in the applicable Subscription Order.

11.16 "**Third Party Software**" means software and services made part of the Subscription Services but authored by a third party.

11.17 "**Users**" means Customer's employees, consultants, agents, contractors, Affiliates, and other third parties that are (i) authorized by Customer to access the Subscription Services on behalf of Customer, or otherwise use the Services for the benefit of Customer, and (ii) provided with (or that Workiva provides at Customer's request) user identifications and passwords to access Customer's account.

IN WITNESS WHEREOF, by signing below the parties agree to be bound by the foregoing Main Terms.

«ACCOUNT_LEGAL_NAME»	workiva
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A
SECURITY STANDARDS

1.0 Workiva Information Security Standards.

1.1 Workiva will maintain a comprehensive information security program ("**Workiva Security Program**") which includes administrative, technical and physical safeguards to protect Customer Data. Workiva safeguards are maintained to protect Customer Data based on commercially reasonable and industry standard resources available to Workiva and the type of the Customer Data. The Workiva Security Program is designed to:

(a) Protect the availability, integrity and confidentiality of Customer Data;

(b) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data;

(c) Protect against any unlawful unauthorized access, unlawful use, disclosure, alteration, or destruction by Workiva of Customer Data; and

(d) Protect against any accidental loss, destruction, or damage to Customer Data.

1.2 Workiva will also monitor, evaluate and modify the Workiva Security Program to ensure:

(a) Use of industry standard technology pertinent to the protection of Customer Data;

(b) Commercially reasonable updates to the Services, Subscription Services, Workiva Security Program or Workiva's systems, based on relevant changes in internal procedures for the protection of Customer Data, or as necessary to comply with applicable law; and

(c) Workiva relevant internal changes to Workiva's technical environment including third parties, outsourcing arrangements, infrastructure and information systems.

2.0 Governance. Workiva will maintain a governance program which includes:

2.1 Compliance with the baseline of security controls for a Software as a Service (SaaS) Cloud Service Provider

2.2 Policies and procedures based on the NIST Cybersecurity Framework, ISO 27001:2022, and other industry standard frameworks;

2.3 Data classification;

2.4 Geo-location options for storage of Customer Data;

2.5 Risk management; and

2.6 Third party security risk management.

3.0 Access Controls. Workiva will maintain policies, procedures and logical controls designed to:

3.1. Limit access to Workiva facilities and systems where those systems are limited to authorized persons;

3.2. Limit Workiva employees' access to Customer Data by enforcing segregation of duties;

3.3. Protect from unauthorized access to Customer Data;

3.4. Remove or restrict Workiva employees' access to Customer Data in a timely manner when access thereto is no longer required to perform Services, or upon Customer request;

3.5. Require multi-factor authentication through Federated Service for Workiva access to Customer Data for the provision of Services; and.

3.6. Maintain a password policy within NIST guidelines (i.e., 12 character minimum with two factor authentication).

4.0 Human Resource Security. Workiva will maintain security and privacy policies and procedures for Human Resource including:

4.1. Performing pre-employment background screening commensurate with such employee's level of access to data, subject to applicable law;

4.1. Requiring all employees sign non-disclosure agreements;

4.2. Annual security and privacy role-based training (including requirements of the Workiva Security Program, the importance of securing Customer Data, and how to diagnose phishing attacks); and

4.3. Promoting a culture of security awareness through periodic training, phishing assessments, blogs and programs which reward security best practices.

5.0 Physical and Environmental Security. Workiva will maintain controls that are designed to protect from unauthorized access and against environmental hazards, including:

5.1. Controlled access to Workiva facilities;

5.2. Inheritance of Physical and Environmental security controls from FedRAMP Moderate compliant Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) CSPs.

5.3. Logging and monitoring of access and unauthorized access to Workiva facilities and systems;

5.4. Camera monitoring of Workiva facilities;

5.5. Temperature, fire protection, humidity monitoring of Workiva facilities; and

5.6. Uninterrupted power supplies to Workiva facilities to maintain normal working conditions in compliance with our Business Continuity Plan.

6.0 Secure Development Lifecycle. Workiva will maintain policies and procedures which will reasonably assure that development is done with commercially reasonable security practices including:

6.1. Secure development policies;

6.2. Secure development training;

6.3. Configuring systems and network devices in accordance with Workiva hardening guidelines;

6.4. Development with code review for releases using tools for Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST);

6.5. Vulnerability management and remediation within policy timelines;

6.6. Segregation of duties for development review and release management;

6.7. Vulnerability testing which includes OWASP Top 10, CWE and SANS Top 25; and

6.8. Workiva has and will maintain a formal change management program with segregation of duties.

7.0 Monitoring. Workiva will provide network, system and application monitoring including servers, disks and Security events for any potential problems designed to:

7.1. Review changes to systems and infrastructure;

7.2. Review changes which handle systems, authentication authorization and auditing;

7.3. Review privileged access to Workiva systems;

7.4. Review access to Workiva production environment including abnormal access; and

7.5. Engage third party vulnerability and penetration testing for Workiva systems environment on a regular basis with a report available for customers.

7.6. Participate in the FedRAMP Continuous Monitoring Program which includes monthly vulnerability scanning and remediation, annual third party assessments and penetration testing.

8.0 Encryption. Workiva will provide reasonable assurance of the protection of Customer Data through encryption algorithms within NIST guidelines, which includes:

8.1. Transmission encryption using a minimum of AES 128 with TLS 1.2;

8.2. Encryption at rest using AES 256; and

8.3. Full disk encryption on all hard drives with access to production data with at least AES 128.

9.0 Incident Response. Workiva will maintain an incident response policy with procedures to provide Customer with reasonable assurances that Workiva can respond to any type of security event or breach, and which includes:

9.1. Roles and responsibilities with a team and a dedicated leader which is tested annually;

9.2. Methods for investigation and escalation assessing the event to determine the risk the event poses including proper escalation;

9.3. Processes regarding internal communications, reporting and notification and external reporting and notification to customers without undue delay, and in any case, where feasible, notify within forty-eight (48) hours of Workiva's discovery of any incident involving the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data (to facilitate timely notification Customer must register and maintain an up-to-date email with notice to security@workiva.com; where no such email is provided, Customer acknowledges that the means of notification shall be at Workiva's reasonable discretion); Appropriate documentation of the event, incident and investigation of what was done and by whom with authorization for later analysis and possible legal action; and

9.4. Creation of appropriate documentation of the incident and performance of an investigation and audit for root cause analysis and remediation with authorization for later analysis and possible legal action, provided, however, Workiva's obligations in this Section 9.4 do not apply to incidents resulting from an act or omission of Customer, including, without limitation, a Customer's failure to maintain the security and confidentiality of User credentials.

10.0 Contingency Planning. Workiva will maintain policies and procedures for the response and or recovery of an emergency or other occurrence either natural or pandemic that could damage or affect systems, and the environment of customer data. Such procedures include:

10.1. Data resiliency through redundancy to recover data;

10.2. Regular data backups, including annual testing of the backup and restoration procedures;

10.3. Business Continuity and Disaster Recovery plan which is communicated and made available within an event to minimize the impact and or loss of vital resources;

10.4. Annual testing of the Business Continuity Plan and Disaster Recovery Plan (Executive Summary available to Customer upon request); and

10.5. Auditing of the Disaster Recovery test.

11.0 Audit and Testing.

11.1. So that Customer can verify Workiva's compliance with the DPA and these Security Standards, upon Customer's request, Workiva shall provide to Customer (at Workiva's expense) the following: (a) Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ); (b) SOC 1 Type II; (c) SOC 2 Type II; (d) ISO/IEC 27001:2022: Certification; (e) Workiva Information Security Policies; and (f) Web Application Vulnerability Assessment and Penetration Testing of Workiva equivalent, non-production environment which includes: (i) network scanning; (ii) improper input handling (e.g., cross site scripting, SQL injections, XML injection, and cross site flashing); (iii) weak session management; (iv) insufficient authentication; (v) insufficient authorization; (vi) data validation flaws and data integrity; (vii) OWASP Top 10; and (viii) CWE/SANS Top 25 (collectively, the "**Reports**").

11.2. If the Reports provided are insufficient to demonstrate Workiva's compliance with the DPA or the Security Standards, at Customer's expense Workiva shall also provide written responses (on a confidential basis) to reasonable requests

for information related to Workiva's processing or security of Customer Data, including responses to information security and audit questionnaires, no more than once in any twelve (12) month period.

11.3. If Customer reasonably demonstrates that the information provided pursuant to Sections 11.1 and 11.2 is insufficient to demonstrate compliance with the DPA or the Security Standards, subject to Section 11.4, Customer may perform at Customer's expense:

(a) An audit in relation to Workiva's processing and security of Customer Data (which may also be performed by Customer's third party auditor, subject to Workiva's reasonable approval) ("**Audit**"); or
(b) A penetration test of an equivalent, non-production environment ("**Pen Test**").

11.4. Following receipt by Workiva of a request arising out of 11.3(a) or 11.3(b), Workiva and Customer shall mutually agree in advance on details of such Audit or Pen Test, including the start date, scope and duration, as well as reasonable conditions designed to mitigate potential risks to confidentiality, security, or other potential disruption of the Service or Workiva's business. Audits, Pen Tests and any information arising therefrom are deemed Workiva's Confidential Information. If Customer discovers any actual or potential vulnerability in connection with a Pen Test, Customer must immediately disclose it to Workiva and shall not disclose it to any third-party except as expressly permitted under the Agreement. Customer shall immediately notify Workiva with information regarding any material noncompliance discovered during the course of an Audit. Customer acknowledges that Audits and Pen Tests will be performed at Customer's own expense, with thirty (30) days advance written notice to Workiva, during normal business hours (unless otherwise mutually agreed upon in advance for Pen Tests), no more than once in any twelve (12) month period, subject to Workiva's reasonable security and confidentiality requirements, and solely to the extent the exercise of rights under Section 11.3 would not infringe Applicable Data Protection Laws.

12.0 Disposal. Workiva has policies and procedures to provide reasonable assurance to the appropriate disposal of Customer Data including:

12.1. Secure shredding of printed documents and Customer Data; and

12.2. Secure destruction of Customer Data with a certificate of destruction provided by Workiva.

13.0 Endpoint Devices. Workiva has policies, procedures and technical controls to protect endpoint devices including:

13.1. Malware protection with automated updates and centralized tracking and management, and regular updates and patches;

13.2. Full Disk Encryption (mitigating control as Customer Data is not stored on endpoint devices);

13.3. Regular updates and patching of the Subscription Services, Workiva's systems and browsers; and

13.4. No write to removable media (USB).

14.0 Malware and Patching. Throughout the Agreement Term and in accordance with standard industry practice, Workiva will:

14.1. Perform regular monitoring for security patches;

14.2. Apply patches in a timely manner after testing through change control; and

14.3. Regularly update systems and networks with new releases.

15.0 Shared Security Model. Customer acknowledges the security of the Subscription Services is a shared responsibility between Workiva and Customer. Technical security, as outlined in this Exhibit, is the responsibility of Workiva. It is the responsibility of Customer to (i) promptly report to Workiva any suspicious activities related to Customer's Subscription Services account (e.g., a user credential has been compromised), and (ii) appropriately configure User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data.

EXHIBIT B
DATA PROCESSING AGREEMENT

1.0 Purpose of the DPA. This DPA is intended to satisfy the requirement for an obligatory contract between Customer and Workiva with regard to Workiva's Processing of Customer Personal Data on behalf of customer in connection with Workiva's provision of Services under the Agreement and in accordance with the requirements of Applicable Data Protection Law. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

2.0 Definitions. For the purpose of this DPA, these terms shall mean the following:

2.1 "Applicable Data Protection Law" shall mean the laws and regulations of the United States, the European Union, the European Economic Area ("**EEA**") and/or their member states, Switzerland, the United Kingdom, and/or Canada as applicable to the Processing of Customer Personal Data as set forth in Section 5.0 of this DPA, including but not limited to, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the United Kingdom Data Protection Act 2018 (collectively the "**UK GDPR**") and the Swiss Federal Act on Data Protection Act ("**FADP**").

2.2 "Authorized Personnel" means (a) Workiva employees and Workiva Affiliates' employees who have a need to know or otherwise access Customer Personal Data for the purposes of performing applicable Services; and (b) Workiva's contractors, agents, and auditors who have a need to know or otherwise access Customer Personal Data to enable Workiva to perform the Services.

2.3 "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

2.4 "Customer Personal Data" means Personal Data that is Customer Data.

2.5 "Data Privacy Framework" or "DPF" means the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF ("**UK Extension**"), and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") as set forth by the U.S. Department of Commerce.

2.6 "Personal Data" means any data relating to an identified or identifiable natural person.

2.7 "Process" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.8 "Processor" means the entity which Processes Personal Data on behalf of the Controller.

2.9 "Personal Data Breach" means a breach of Workiva's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed.

2.10 "Standard Contractual Clauses" or "SCCs" means the clauses for the transfer of Personal Data from the EEA to non-EEA countries that do not provide an adequate level of data protection approved by European Commission Decision of 4 June 2021, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

2.11 "Sub-processor" means a Workiva Affiliate or authorized third party service provider engaged by Workiva in the provision of Services under the Agreement and Processes Customer Personal Data. Sub-processors include Workiva Affiliates: https://www.workiva.com/legal/support-affiliates and third party service providers: https://www.workiva.com/legal/sub-processors.

2.12 "Supervisory Authority" means any data protection authority defined under Applicable Data Protection Law.

2.13 "UK Data Transfer Addendum" means the international data transfer addendum to the Standard Contractual Clauses approved by the UK Information Commissioner's Office, as currently set out at: https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf.

3.0 Processing of Customer Personal Data.

3.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data under the Agreement, Customer is a Controller or a Processor, Workiva is a Processor, and that Workiva or Workiva Affiliates will engage Sub-processors pursuant to Section 7 of this DPA.

3.2 Workiva as a Processor. As between the parties, all Customer Personal Data Processed by Workiva on behalf of Customer under the terms of the Agreement shall remain the property of Customer. During the Agreement Term, Workiva shall Process Customer Personal Data in accordance with Customer's written instructions and as permitted in the Agreement and this DPA. To the extent such Customer Personal Data is not so categorized on the applicable Order, SOW or otherwise in writing, Customer Personal Data and business purposes of Processing are as set forth in Section 5 of this DPA. Customer Personal Data may be Processed by

Workiva and its Sub-processors in the EEA, UK, and any other locations around the world provided that the transfer of Customer Personal Data comply with this DPA and Applicable Data Protection Law. If Workiva reasonably believes there is a conflict with any Applicable Data Protection Law and Customer's instructions, Workiva will immediately inform Customer and the parties shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction. Where required under the relevant Applicable Data Protection Law, Workiva shall maintain a record of all Processing activities carried out on Customer Personal Data on behalf of Customer in accordance with Applicable Data Protection Law. Workiva's data privacy team can be contacted via email at privacy@workiva.com.

3.3 Data Subject Requests; DPIAs; Prior Consultations. Workiva shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as permitted); and (ii) any other correspondence, enquiry or complaint received from a data subject, Supervisory Authority or other third party in connection with Workiva's Processing of the Customer Personal Data under the Agreement. If any such request, correspondence, enquiry or complaint is made directly to Workiva, Workiva shall promptly inform Customer by providing full details of the same unless otherwise prohibited. Workiva shall not rectify, erase, restrict, or respond to a data subject request itself, except that Customer authorizes Workiva to redirect the data subject request as necessary to allow Customer to respond directly. Workiva shall provide Customer with reasonable assistance (at Customer's expense) in support of a data protection impact assessment or prior consultation with any Supervisory Authority, solely in relation to Customer Personal Data, the Services and where the Customer would not otherwise have access to the relevant information.

3.4 Return or Deletion. Upon expiration or termination of the Agreement, at Customer's option, Workiva shall return or delete Customer Personal Data pursuant to Section 5.4 (Return and Destruction) of the Main Terms, except where Workiva is required to retain Customer Personal Data by applicable law. Until Customer Personal Data is returned or deleted, Workiva shall continue to comply with this DPA.

3.5 Customer Obligations. Customer shall ensure that its instructions comply with Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of (i) the Customer Personal Data provided to Workiva by or on behalf of Customer; (ii) how Customer acquired any such Customer Personal Data; and (iii) the instructions it provides to Workiva regarding the Processing of such Customer Personal Data. Customer represents and warrants that it has obtained all necessary consents and authorizations required under Applicable Data Protection Law to permit the Processing of Customer Personal Data and international transfer of Customer Personal Data (where applicable) from Customer to Workiva.

4.0 Transfer of Customer Personal Data.

4.1 Cross-border Transfer. Workiva shall only transfer Customer Personal Data outside the EEA, Switzerland or the UK if it has taken necessary measures to ensure the transfer is compliant with the Applicable Data Protection Laws and this DPA.

4.2 Transfer Mechanisms. Transfer mechanisms may include (without limitation) transferring Customer Personal Data to a recipient: (a) in a country deemed by the European Commission, the Swiss FDPIC, the UK Secretary of State or the UK GDPR as providing adequate protection for Personal Data, including a transfer pursuant to the (i) EU-US DPF, and/or (ii) the UK Extension of the EU-US DPF, (b) that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, (c) that has executed to the extent required the applicable standard contractual clauses adopted or approved by the European Commission, the Swiss FDPIC or approved by the UK ICO. Workiva has executed the Standard Contractual Clauses with its Sub-processors where applicable, and Customer shall be deemed a third party beneficiary of the Standard Contractual Clauses. For the sake of clarity, the data subject may enforce directly the provisions of the Standard Contractual Clauses.

4.3 Data Privacy Framework. Workiva's U.S. entity (Workiva Inc.) and applicable Sub-processors are certified under the Data Privacy Framework. Customer may validate such certificates by accessing https://www.dataprivacyframework.gov/.

4.4 Alternative Transfer Mechanism. If Workiva adopts an alternative data export mechanism approved and authorized by the relevant EU, Swiss, or UK authorities (including any new version of or successor to the Standard Contractual Clauses, Binding Corporate Rules, or Data Privacy Framework principles adopted pursuant to Applicable Data Protection Law) for the transfer of Personal Data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with the GDPR, UK GDPR, and/or Swiss FADP and extends to the territories to which Personal Data is transferred).

5.0 Description of Processing. The parties agree to the following description of Processing with regard to Workiva's Processing of Customer Personal Data pursuant to the Agreement:

5.1 Categories of Data Subject. Employees and contractors of Customer, and Customer's Users whose Personal Data is provided by Customer to Workiva for the purpose of accessing and using the Subscription Services in accordance with the Agreement.

5.2 Categories of Personal Data. Customer Personal Data provided by Customer and processed by Workiva in the course of providing the Services, and User identification data such as business contact information (e.g., name, email address, phone number), and IP address.

5.3 Special Categories of Data. There are no special categories of data or sensitive Personal Data being Processed.

5.4 Nature of Processing. Customer Personal Data Processed by Workiva under the Agreement may be subject to the following Processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, consult, use, align or combine, block, erase or destruct, disclose by transmission, disseminate or otherwise make available Customer Personal Data as described herein, as necessary for Workiva to provide the Services and otherwise in accordance with Customer's instructions.

5.5 Purpose of Processing. Customer instructs Workiva to Process Customer Personal Data for the following purposes: (a) to provide Services to Customer in accordance with the Agreement; (b) Processing of Users' e-mail addresses to provide log-in credentials; (c) Processing of Users' log-in credentials and IP address for authentication purposes and to provide Users access to the Subscription Services in accordance with the Agreement; (d) Processing of Users' contact information and IP address to provide Support; and (e) hosting and storage of Customer Data that contains Customer Personal Data.

6.0 Security Controls. Workiva shall maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Customer's data and confidential and proprietary information, including Customer Personal Data, as further set forth in Workiva's "Security Standards" (as set forth in Exhibit A to the Main Terms). Workiva declares that its Security Standards are in line with GDPR Article 32. Workiva will regularly monitor compliance with the Security Standards. Workiva will not intentionally decrease the Security Standards during the Agreement Term.

7.0 Sub-processors.

7.1 Customer acknowledges and authorizes Workiva's use of its Sub-processors existing as of the Effective Date as set forth in Section 7.4 below. Customer hereby gives general authorization to new or replacement Sub-processors, provided Workiva follows the following procedure:

(a) With respect to any new or replacement Sub-processor Workiva shall (i) execute a written agreement that obligates it to (1) protect such Customer Personal Data to the same extent as is required of Workiva by the Agreement, and (2) be in compliance with Applicable Data Protection Laws, and (ii) ensures such new Sub-processor is subject to industry-standard external security auditing (collectively, the "**Conditions**").

(b) Workiva agrees to provide Customer with notice at least thirty (30) days in advance of engaging any new or replacement Sub-processors to Process Customer Personal Data under the Agreement ("**Sub-processor Notice**") giving the Customer the opportunity to object. Such Sub-processor Notice may be provided by sending an email to the Account Administrator indicated in the applicable Order. The Sub-processor Notice shall include the name of the new or replacement Sub-processor, the services such Sub-processor will provide under the Agreement, and the geographic locations where Customer Personal Data will be Processed. Where applicable and upon Customer's request, Workiva agrees to provide a transfer impact assessment pursuant to Clause 14 of the SCCs and a copy of the SCCs executed by Workiva and the Sub-processor.

(c) If Customer has a reasonable belief that such new Sub-processor cannot comply with the Conditions, Customer may provide written notice to Workiva within twenty (20) days of being informed of the engagement of the new Sub-processor, and the parties agree to work in good faith to resolve such issues. If such issues cannot be resolved, Customer may object to any new Sub-processor by terminating the applicable Order(s) with respect only to those services which cannot be provided by Workiva without the use of the objected-to new Sub-processor. Such termination will be made by providing written notice to Workiva. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Sub-processor. For the avoidance of doubt, Customer will be deemed to have consented to such Sub-processor absent an objection within the stated time period.

(d) Customer acknowledges that Workiva provides a standardized service to all customers which does not allow using different Sub-processors for different customers and, therefore, that the inability to use a particular new or replacement Sub-processors for the Services to the Customer may result in delay in performing the Services, inability to perform the Services or increased fees. Workiva will notify Customer in writing of any change to Services or fees that would result from Workiva's inability to use a new or replacement Sub-processors to which Customer has objected.

7.2 Workiva may replace a Sub-processor without advance notice where the reason for the change is outside of Workiva's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Workiva will inform Customer of the replacement Sub-processor as soon as possible following its appointment. Section 7.1 applies accordingly.

7.3 Workiva shall be liable for the acts and omissions of its Sub-processors to the same extent Workiva would be liable if performing the Services of each Sub-processors directly under the terms of this DPA.

7.4 A current list of Workiva's Sub-processors as may be used for Processing Customer Personal Data is available to Customer without charge on Workiva's website (Workiva Affiliates: https://www.workiva.com/legal/support-affiliates; third party Sub-processors: https://www.workiva.com/legal/sub-processors). Workiva will keep the Sub-processors list current and inclusive of any new sub-processors and will make available to Customer the updated Sub-processors list upon request by Customer.

8.0 Personal Data Breaches. After becoming aware of a Personal Data Breach Workiva will (a) notify Customer of the Personal Data Breach without undue delay; (b) investigate the Personal Data Breach; (c) provide Customer with details about the Personal Data Breach; and (d) make reasonable efforts to prevent a recurrence of the Personal Data Breach. Workiva agrees to cooperate in Customer's handling of the matter by: (i) providing reasonable assistance with Customer's investigation; and (ii) making available relevant records, logs, files, data reporting, and other materials related to the Personal Data Breach's effects on Customer, as required to comply with Applicable Data Protection Law. Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

9.0 Authorized Personnel. Workiva employees and employees of its Authorized Personnel that have access to Customer Personal Data are subject to appropriate background check procedures as further set forth in the Security Standards. If, in the Customer's reasonable and good faith opinion, one or more of Workiva's employees, or employees of its Authorized Personnel, poses a risk to the security of such Customer Personal Data, Workiva will immediately terminate access by such individuals and assign different and qualified individuals. Workiva will ensure that its Authorized Personnel who are engaged in the Processing of Customer Personal Data under the Agreement have committed themselves to confidentiality and have received adequate training and instruction to allow them to comply with the terms of this DPA.

10.0 Audits. The parties agree that any audits regarding Workiva's compliance with the obligations set forth in this DPA, shall be conducted in accordance with Section 11 of Exhibit A to the Main Terms.

11.0 Government Access Requests. To the extent that Workiva receives a request from a relevant government authority responsible for national security and intelligence gathering ("**Government Authority**") to access Customer Personal Data in accordance with applicable law (including the Foreign Intelligence Surveillance Act), Workiva shall: (a) inform Customer of the request to the extent permitted by applicable law so that Customer may take all protective measures or action as appropriate, and Workiva agrees to provide reasonable assistance should it be required during the course of the procedure; and (b) disclose the requested data to the Government Authority without liability if applicable laws prohibit notification of the request to third parties, provided that Workiva shall furnish only such portion of the information that is legally required to be disclosed and only to the extent required by applicable law. For the avoidance of doubt, nothing in this DPA shall require Workiva to pursue action or inaction that could result in civil or criminal penalty for Workiva such as contempt of court.

12.0 Interpretation. The parties agree that when interpreting Applicable Data Protection Law in conjunction with each party's rights and obligations in this DPA, it shall be interpreted based on the applicable party's role in its Processing of Customer Personal Data.

13.0 Miscellaneous.

13.1 Conflicts. In the event of any conflict or inconsistency between this DPA and the Agreement, the terms of this DPA shall prevail.

13.2 Severability. In the event any provision of this DPA, in whole or in part, is invalid, unenforceable or in conflict with the applicable laws or regulations of any jurisdiction, such provision will be replaced, to the extent possible, with a provision which accomplishes the original business purposes of the provision in a valid and enforceable manner, and the remainder of this DPA will remain unaffected and in full force.

13.3 Liability. Each party's and such party's Affiliates' liability, taken together in the aggregate, for breaches of this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement.