ATTACHMENT 1

EXHIBIT C - MANUFACTURER COMMERCIAL TERMS AND CONDITIONS ADDENDUM

Workiva End User Agreement
GSA Approved – October 8, 2025

THIS WORKIVA END USER AGREEMENT ("**AGREEMENT**") BETWEEN AGENCY AND WORKIVA COVERS AGENCY'S ACCESS AND USE OF THE SERVICES. AGENCY AGREES TO BE BOUND BY THIS AGREEMENT THROUGH (1) AGENCY'S EXPRESS AGREEMENT TO THE TERMS AND CONDITIONS SET FORTH HEREIN, OR (2) AGENCY'S USE OF THE SERVICES. IF YOU DO NOT HAVE AUTHORITY TO ENTER INTO THIS AGREEMENT OR YOU OR AGENCY DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, THEN DO NOT USE THE SERVICES.

1.0 Services

1.1 Subscription Services.

(a) **Usage Access**. Workiva will provide Agency with Usage Access pursuant to the terms of this Agreement. During the Subscription Term, subject to the terms of this Agreement, Workiva grants to Agency 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. Agency and its Users may access and use the Subscription Services pursuant to a Subscription Order..

(b) **Users**. Agency may not allow Users to access the Subscription Services on a shared user basis, however, Agency may reassign different individuals on a reasonable basis. Agency is responsible for each of its Users' acts and omissions and remains liable to Workiva for any User's breach of this Agreement.

(c) **Updates; System Requirements**. Workiva may update features, functionality, software, or user types that Agency accesses pursuant to an active Order; provided that such updates will be at no cost to Agency and will not materially degrade existing features and functionality. Agency 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**"). The Minimum System Requirements are set forth in the Documentation.

(d) **Usage Restrictions**. Agency 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 9.4 - Assignment), lease, rent, sublicense, or otherwise transfer or make available the rights granted to Agency under this 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 in the Subscription Services; (h) use the 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 the Subscription Services or third party data contained therein; or (j) gain or attempt to gain unauthorized access to any portion of the Subscription Services (including any application programming interfaces in the Subscription Services), or its related systems or networks, for use in a manner that would exceed the scope granted under this Agreement, or facilitate any such unauthorized access for any third party. If any unauthorized access occurs, Agency shall promptly notify Workiva of the incident and shall reasonably cooperate in resolving the issue.

(e) Order Compliance. Workiva reserves the right to verify Agency compliance with the scope and terms of a Subscription Order. If Workiva determines that Agency is out of compliance with a Subscription Order, Workiva will provide written notice to Agency or its Authorized Provider regarding such non-compliance. Agency shall have thirty (30) days from receipt of such notice to cure such non-compliance. If Agency fails to cure its non-compliance within the thirty (30) day period, Workiva may: (1) suspend Agency's Services, and/or (2) terminate the applicable Order(s).

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

2.0 Security; Agency Data.

2.1 Security and Data Privacy. Workiva shall maintain appropriate administrative, physical, and technical safeguards to protect the security, confidentiality and integrity of Agency Data, as described in Workiva's security standards set forth in Exhibit A

(Security Standards). To the extent Agency Data includes Personal Data, Workiva represents and warrants to only process such data pursuant to Agency's requests or as set forth in Exhibit B (Data Processing Agreement or DPA).

2.2 Agency Data; Responsibilities. Except as otherwise provided in this Agreement (or instructed by Agency), Workiva shall only process Agency Data to provide the Services. Workiva will neither have the responsibility to review, nor any liability as to the accuracy or integrity of, any information or content posted by Agency or its Users. Agency is responsible for any consents or government authorizations necessary for the collection, use and disclosure of all Agency Data in its use of the Subscription Services.

2.3 Usage Data. Notwithstanding anything contrary in this Agreement, Workiva may collect, store and use the 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. Subject to Section 4 (Confidentiality), Workiva may share Usage Data with third parties to the extent it is aggregated and anonymized such that Agency and its Users cannot be identified. Workiva will be the owner of any intellectual property generated through Workiva's use of such Usage Data. Workiva may utilize the services of third party service providers to collect, store and use such Usage Data, and Workiva shall be responsible for such third party service providers' compliance with this Agreement as they relate to the collection, storage and use of Usage Data on behalf of Workiva.

3.0 Term; Termination.

3.1 Term

(a) **Agreement Term**. The Agreement begins on the date Agency enters into an agreement and a Subscription Order with an Authorized Provider that references this Agreement and shall continue until all Orders associated with the Agreement have expired or have otherwise been terminated (the "**Agreement Term**").

(b) **Subscription Term**. The Subscription Services will begin on the start date (as defined in the 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 an Order which will control in cases of conflict with this Section.

(c) **SOW Term**. The period of performance for Professional Services will be as agreed upon in the SOW.

3.2 **Termination**. The provisions of this Agreement will continue in effect following termination of your subscription for the Services. Upon expiration or termination of a Subscription Order and/or the Agreement, Agency must stop using the applicable Subscription Services.

4.0 Confidentiality

4.1 Confidential Information. During the Agreement Term each party may disclose Confidential Information. Except as otherwise agreed in writing, each party agrees that: (a) all information communicated to it by the other in connection with this Agreement and identified as confidential, (b) any information exchanged between the parties in connection with Agency's purchase of any additional Services (including information related to future business relationships or Services not currently addressed under this Agreement, such as requests for proposals, bids, correspondence, negotiations, and discussions), (c) the terms of this Agreement, and (d) all information communicated to receiving party that a reasonable person would have understood to be confidential to the disclosing party, will be Confidential Information. Workiva Confidential Information includes the Services, development plans, and any security specifications, reports or assessments related to the Services, Workiva or its licensors and third parties. Agency Confidential Information includes Agency Data.

4.2 Standard of Care; Third Parties. Each party will use at least the same degree of care to safeguard the Confidential Information of the other party as it employs for its own information (or information of its Agencys) of a similar nature, and in any event, no less than reasonable care. Each party may disclose the other party's Confidential Information to employees, consultants, contractors, advisors and other third parties provided that such parties are subject to written confidentiality obligations at least as restrictive as those set forth in this Agreement (or other professional or fiduciary obligations of confidentiality), and have a need to know. Each party will be responsible for any improper disclosure of Confidential Information by such party's employees, agents, or contractors.

4.3 Restrictions. Neither party will (a) use, or make any copies of, the Confidential Information of the other party except to fulfill its rights and obligations under this Agreement, (b) acquire any right in or assert any lien against the Confidential Information of the other, or (c) sell, assign, lease, or otherwise commercially exploit the Confidential Information (or any derivative works thereof) of the other party. Neither party may withhold the Confidential Information of the other party or refuse for any reason (including due to the other party's actual or alleged breach of this Agreement) to promptly return to the other party its Confidential Information (including copies thereof) if requested to do so.

4.4 Return and Destruction. Upon expiration or termination of this Agreement and completion of a party's obligations under this Agreement, each party will return or destroy, as the other party may direct, the other party's Confidential Information. Workiva will fulfill the obligation to return Agency 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 Agency Data in the file formats set forth in the Documentation (e.g., EDGAR, DOCX, CSV, Excel, PDF). 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.

4.5 Exclusions; Permitted Use. This Section 4 will not apply to any information that either party can demonstrate (a) was, at the time of disclosure to it, 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 the 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 the receiving party without use of the Confidential Information of the disclosing party. In addition, a party will not be considered to have breached its obligations under this Section 4 for disclosing Confidential Information of the other 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 it is legally permissible, such party advises the other party prior to making such disclosure and provides a reasonable opportunity to the other 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.

4.6 Unauthorized Access. Each party will: (a) notify the other party promptly of any material unauthorized possession, use, disclosure, or knowledge of the other party's Confidential Information that becomes known to such party, (b) promptly furnish to the other party details of the unauthorized possession, use, disclosure, or knowledge, or attempt thereof, and use reasonable efforts to assist the other 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 the other party in any litigation and investigation against third parties deemed necessary by the other 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.

5.0 Ownership; Feedback.

5.1 Workiva Ownership. Workiva (or its licensors) retains all ownership of and title to, and 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. Agency acknowledges and agrees that 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 Agency. Agency shall acquire no rights therein other than those limited rights of use specifically conferred by this Agreement. All rights related to the Services that are not expressly granted to Agency under this Agreement are reserved by Workiva (or its licensors).

5.2 Agency Ownership. As between Workiva and Agency, Agency is, and will remain, the owner of all Agency Data. Workiva will only process Agency Data to provide the Services and in accordance with this Agreement or as otherwise permitted by Agency in writing. Workiva acquires no right, title, or interest from Agency or its Users to Agency Data, including any intellectual property rights therein. Any reports or documents generated through Agency's use of the Subscription Services in accordance with this Agreement will be owned by Agency. If such reports or documents include any pre-existing intellectual property owned by Workiva, Workiva hereby grants to Agency a worldwide, perpetual, nonexclusive, royalty-free 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 Agency's reports or documents.

5.3 Feedback. If Agency or its Users provides Workiva with Feedback, Agency hereby grants Workiva a perpetual, irrevocable, royalty-free, fully paid-up, worldwide license to use such Feedback, and Workiva has the right, but not the obligation, to use such Feedback in any way without restriction or obligation to Agency. Workiva will be the exclusive owner of any modifications, enhancements, or derivative works of the Services resulting from Workiva's use of such Feedback.

6.0 Warranties; Disclaimers.

6.1 Mutual Representations and Warranties. Each party represents and warrants that: (a) it has, and throughout this Agreement Term, will retain, the full right, power, and authority to enter into this Agreement and perform its obligations hereunder, (b) the acceptance of this 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 this Agreement will constitute the legal, valid, and binding obligation of such party, enforceable in accordance with its terms.

6.2 Workiva Representations and Warranties. Workiva warrants: (a) that the Subscription Services will perform materially in accordance with the Documentation and this Agreement, (b) to use commercially reasonable efforts to correct material defects that are reported by Agency or its Users, (c) the Services will be performed 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 this Agreement, (d) the Documentation will be reasonably updated so that it continues to describe the Subscription Services and Services in all material respects, and (e) to the best of its knowledge, the Subscription Services do not contain code whose purpose is to disrupt, damage, or interfere with Agency systems, software, or Agency Data. Agency 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 6.2, Agency must remain in compliance with the Minimum System Requirements.

6.3 Compliance with Laws.

(a) Each party represents and warrants that it shall at all times comply with all applicable regulations and good business practices when performing its duties under this Agreement, and that it shall take no action nor make payment that may constitute a violation of the foregoing.

(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 this Agreement in accordance with Section 3.2 (Termination) without any further obligation or liability hereunder.

(c) Workiva's 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**"). The parties agree to comply with all applicable export and import laws and regulations. Agency acknowledges that the Services may not be exported or re-exported to any countries on the Sanctions List. The Sanctions Lists are subject to change from time to time without notice and limitation. Workiva reserves the right and shall not be liable for blocking Users' access if they are located in any embargoed countries. In addition, Workiva may immediately suspend a User if Workiva discovers that such a User is subject to the Sanctions' Lists. Agency represents and warrants that Agency and any Agency director, officer, agent, employee, affiliate or other person associated with or acting on Agency's behalf or any of its affiliates or subsidiaries is not located in any such country or on any such list.

(d) 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. Agency agrees that Agency will not use the Services for any purposes prohibited by U.S. law, including terrorism, the development, design, manufacture, or production of missiles, or for development of nuclear, chemical, or biological weapons.

6.4 Agency Acknowledgments. As between the parties, Agency is solely responsible for obtaining all necessary rights and consents to enter Agency Data into the Subscription Services. Agency hereby represents and warrants that (a) Agency has sufficient rights to provide Agency Data to Workiva under this Agreement, and (b) Agency Data will not violate or infringe the rights of any third party. Agency further acknowledges that neither Workiva nor the Subscription Services is a primary system of record of Agency Data, and Agency 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 Agency hardware or software, Workiva will so inform Agency and it will be Agency's responsibility to obtain and pay for any required repairs or modifications.

6.5 DISCLAIMERS.

(a) EXCEPT AS SPECIFICALLY SET FORTH IN THE AGREEMENT, TO THE FULLEST EXTENT PERMITTED BY LAW, THE SUBSCRIPTION SERVICES AND SERVICES ARE PROVIDED "AS IS." WORKIVA, ITS LICENSORS, AND SERVICE PROVIDERS DO NOT MAKE 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, AND WORKIVA EXPRESSLY DISCLAIMS ANY AND ALL SUCH WARRANTIES TO THE FULLEST EXTENT PERMITTED BY LAW.

(b) Workiva does not warrant that the Subscription Services: (i) will be uninterrupted or error free; or (ii) 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.

(c) Agency acknowledges and agrees that Workiva and its licensors are not responsible for: (i) the performance of Agency'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 Agency's or its Users' connection to the internet, and Agency acknowledges that the Subscription Services may be subject to limitations, delays, and other problems inherent in the use of such communications facilities.

7.0 Infringement Indemnification.

7.1 Workiva Indemnification. Workiva will: (a) defend Agency from and against any claim by a third party alleging that the Subscription Services, when used as authorized under this Agreement, infringes such third party's patents, copyrights, or trademarks, and (b) in relation to such claim, indemnify and hold harmless Agency 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).

7.2 Agency Indemnification. Agency will: (a) defend Workiva from and against a claim by a third party alleging that any Agency Data infringes such third party's patents, copyrights, or trademarks, and (b) in relation to such claim, indemnify and hold harmless Workiva from any damages and costs awarded by a court or agreed to in settlement by Agency (including reasonable attorneys' fees).

7.3 Procedures for Indemnification. The indemnifying party's ("**Indemnitor**") obligations under Section 7.1 or 7.2 are expressly conditioned on the following: the party seeking indemnification ("**Indemnitee**") shall (a) promptly notify 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) in writing, grant Indemnitor sole control of the defense of any such claim and of all negotiations for its settlement or compromise, provided that no such settlement or compromise may impose any monetary or other obligations on Indemnitee, and (c) reasonably cooperate with Indemnitor to facilitate the settlement or defense of the claim.

7.4 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 (i) procure for Agency, at no additional cost to Agency, the right to continue to use the Subscription Services, (ii) replace or modify the Subscription Services, at no cost to Agency, to make it non-infringing, provided that the same function is performed by the replacement or modified Subscription Services, or (ii) if in Workiva's judgment the aforementioned "(i)" and "(ii)" are not commercially feasible, terminate this Agreement (or the applicable Order) and grant Agency a pro-rated refund of any advance Fees paid applicable to the remainder of the Subscription Term.

7.5 Combination. Workiva shall have no obligation under the foregoing with respect to: (i) 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, (ii) any claim that arises from Agency's non-compliance with Section 1.1(d) – Usage Restrictions, or (iii) any claim which would not have occurred but for Agency's modification.

7.6 Limitation. This Section 7 states the entire liability of Indemnitor with respect to third party infringement arising from the Services, Software, or Agency Data, or any parts thereof, and Indemnitor shall have no additional liability with respect to any alleged or proven infringement.

8.0 Disclaimer of Certain Damages and Limitation of Liability.

8.1 **DISCLAIMER OF CERTAIN DAMAGES**. EXCEPT AS SET FORTH IN THIS SECTION 8.0, 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.

8.2 **LIMIT ON LIABILITY**. EACH PARTY'S AGGREGATE LIABILITY UNDER THIS AGREEMENT SHALL BE LIMITED TO THE ACTUAL AMOUNT PAID OR PAYABLE BY AGENCY 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 4 (CONFIDENTIALITY), THE SECURITY STANDARDS, AND THE DPA SHALL BE LIMITED TO AN AMOUNT EQUAL TO TWO TIMES (2X) THE ACTUAL AMOUNT PAID OR PAYABLE BY AGENCY DURING THE TWELVE (12) MONTHS PRIOR TO SUCH CLAIM(S) FOR THE SPECIFIC SERVICE(S) GIVING RISE TO SUCH CLAIM(S). BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO AGENCY. NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS SECTION SHALL BE DEEMED TO IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF, OR RELATED TO, THIS

AGREEMENT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31. U.S.C. §§ 3729-3733.

8.3 **Exclusions to the Limitation on Liability**. The limitations in Sections 8.1 and 8.2 shall not apply to: (a) either party's indemnity obligations set forth in Section 7, (b) either party's gross negligence, fraud, criminal acts or willful misconduct, and (c) liability arising out of Agency's obligations under Section 1.1(d).

9.0 Miscellaneous.

9.1 Notice. Any notice or demand which is required to be given under this 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.

9.2 Governing Law. This Agreement shall be governed by and construed under the federal laws of the United States.

9.3 US Government End Users. The Services are deemed to be "commercial computer software" and "commercial computer software documentation" pursuant to FAR 12.212 and DFARS 227.7202. All US Government end users purchase and/or access the Services with only those rights set forth in this Agreement. Any provisions that are inconsistent with federal procurement regulations are not enforceable against the US Government.

9.4 Assignment. Neither party may assign this Agreement, or any of its interest 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 this 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. This Agreement applies to and binds the permitted successors and assigns of the parties.

9.5 Force Majeure. Neither party will be in default or otherwise liable for any delay in or failure of its performance under this Agreement if such delay or failure arises due to any reason beyond its 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 (each, a "**Force Majeure Event**"). The parties will promptly inform and consult with each other as to any of the above causes which in their judgment may or could be the cause of a delay in the performance of this Agreement.

9.6 Injunctive Relief. Each party acknowledges and agrees that a breach, including an anticipatory or threatened breach, by either party of its obligations under this Agreement may cause immediate and irreparable harm to the non-breaching party for which monetary damages may not constitute an adequate remedy. Accordingly, the breaching party acknowledges and agrees that 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 this Agreement, but shall be in addition to all other remedies available to the non-breaching party at law or in equity.

9.7 Third Parties. Based on the particular Services being provided, certain third party pass-through terms may be required to be accepted by Agency. Such third party terms will take precedence in cases of conflict with this Agreement. No other third party will be a beneficiary of this 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 this Agreement caused by such third parties.

9.8 Survival. Without limiting the foregoing, the respective rights and obligations of the parties under Sections 4, 5, 6, 7, 9, and 10 of this Agreement will survive the expiration or termination of this Agreement regardless of when such termination becomes effective.

9.9 Waiver. Failure by either party to enforce any right under this Agreement will not waive that right.

9.10 Severability. If any portion of this Agreement is not enforceable, it will not affect any other terms.

9.11 Order of Precedence. The following order of precedence will be followed in resolving any inconsistencies between the terms of this Agreement and the terms of any Orders, exhibits, statements of work, or other documents: first, this Agreement, second, any terms contained in an Order; and third, the terms of any other documents referenced in any of the foregoing.

9.12 General. This Agreement is the complete agreement between the parties regarding its subject matter and supersedes all prior or contemporaneous communications, understandings or agreements (whether written or oral). This Agreement will not be construed against either party as the purported drafter. With the exception of any terms or conditions that have been accepted or acknowledged (electronically or otherwise) by Agency or a User via Workiva's website or the Subscription Services, no changes in or additions to this Agreement will be recognized unless incorporated herein by amendment, or as mutually agreed in an Order, and signed by duly authorized representatives of both parties.

10.0 Definitions

10.1 "**Authorized Provider**" means Workiva or a Workiva Partner.

10.2 "**Confidential Information**" is information that relates to the disclosing party's or disclosing party's Agencys' business operations, financial condition, customers, products, services, or technical knowledge.

10.3 "**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.

10.4 "**Agency**" means the legal entity acquiring Usage Access upon acceptance of the Agreement.

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

10.6 "**Feedback**" means any comments, suggestions, or other feedback provided by Agency or its Users regarding the Services.

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

10.8 "**Order**" refers to an ordering document for either Subscription Services or Professional Services entered into between Agency and an Authorized Provider.

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

10.10 "**Services**" means Subscription Services and Professional Services, collectively.

10.11 "**Statement of Work**" or "**SOW**" means an ordering document for Professional Services entered into between Agency and an Authorized Provider.

10.12 "**Subscription Order**" means an ordering document for Subscription Services entered into between Agency and an Authorized Provider.

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

10.14 "**Third Party Software**" means software and services made part of the Subscription Services but authored by a third party, including, Google and Amazon Web Services.

10.15 "**Usage Access**" means Agency access to the Subscription Services.

10.16 "**Usage Data**" is any data (other than Agency Data) relating to or derived from the operation or Agency's usage of the Services.

10.17 "**Users**" means employees of Agency, Agency affiliates or third parties of Agency that are provided with (or that Workiva provides at Agency's request) user identifications and passwords to Agency's account. Users may include consultants, contractors, agents, and third parties with which Agency, or an Agency affiliate, transacts business.

10.18 "**Workiva**" means the Workiva entity named in an agreement entered into between Agency and an Authorized Provider and/or an Order.

10.19 "**Workiva Partner**" means a Workiva authorized reseller, distributor or systems integrator authorized by Workiva to sell the Services.

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 Agency Data. Workiva safeguards are maintained to protect Agency Data based on commercially reasonable and industry standard resources available to Workiva and the type of the Agency Data. The Workiva Security Program is designed to:

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

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

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

(d) Protect against any accidental loss, destruction, or damage to Agency 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 Agency 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 Agency 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 Agency 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 Agency Data by enforcing segregation of duties;

3.3 Protect from unauthorized access to Agency Data;

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

3.5 Require multi-factor authentication through Federated Service for Workiva access to Agency 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;

4.2 Requiring all employees sign non-disclosure agreements;

4.3 Annual security and privacy role-based training (including requirements of the Workiva Security Program, the importance

of securing Agency Data, and how to diagnose phishing attacks); and

4.4 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 Agency 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 Agency 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 Agency Data (to facilitate timely notification Agency must register and maintain an up-to-date email with notice to security@workiva.com; where no such email is provided, Agency 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 Agency, including, without limitation, a Agency'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 Agency upon request); and

10.5 Auditing of the Disaster Recovery test.

11.0 Audit and Testing.

11.1 So that Agency can verify Workiva's compliance with the DPA and these Security Standards, upon Agency's request, Workiva shall provide to Agency (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 Agency'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 Agency Data, including responses to information security and audit questionnaires, no more than once in any twelve (12) month period.

11.3 If Agency 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, Agency may perform at Agency's expense:

(a) An audit in relation to Workiva's processing and security of Agency Data (which may also be performed by Agency'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 Agency 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 Agency discovers any actual or potential vulnerability in connection with a Pen Test, Agency must immediately disclose it to Workiva and shall not disclose it to any third-party except as expressly permitted under the Agreement. Agency shall immediately notify Workiva with information regarding any material noncompliance discovered during the course of an Audit. Agency acknowledges that Audits and Pen Tests will be performed at Agency'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 Agency Data including:

12.1 Secure shredding of printed documents and Agency Data; and

12.2 Secure destruction of Agency 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 Agency 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. Agency acknowledges the security of the Subscription Services is a shared responsibility between Workiva and Agency. Technical security, as outlined in this Exhibit, is the responsibility of Workiva. It is the responsibility of Agency to (i) promptly report to Workiva any suspicious activities related to Agency'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 Agency 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 Agency and Workiva with regard to Workiva's Processing of Agency 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 Agency Personal Data as set forth in **Attachment 1** 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**"), the Swiss Federal Act on Data Protection ("**FADP**"), and the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100-.199, as amended by the California Privacy Rights Act of 2020 ("**CCPA**").

2.2 "Authorized Personnel" means (a) Workiva employees and Workiva Affiliates' employees who have a need to know or otherwise access Agency 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 Agency 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 "Agency Personal Data" means Personal Data that is Agency 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, as set out at: https://www.dataprivacyframework.gov/.

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, Agency Personal Data transmitted, stored or otherwise Processed**.**

2.10 "Sell", "Share", and "Service Provider" shall have the same meaning as the terms are defined in the CCPA.\

2.11 "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 the European Commission Implementing Decision of 4 June 2021, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914.

2.12 "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 Agency 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.

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

2.14 "UK Data Transfer Addendum" means the international data transfer addendum to the Standard Contractual Clauses approved by the UK Information Commissioner's Office as set forth in **Attachment 2** of this DPA.

3.0 Processing of Agency Personal Data.

3.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Agency Personal Data under

the Agreement, Agency 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 Agency Personal Data Processed by Workiva on behalf of Agency under the terms of the Agreement shall remain the property of Agency. During the Agreement Term, Workiva shall Process Agency Personal Data in accordance with Agency's written instructions and as permitted in the Agreement and this DPA. To the extent such Agency Personal Data is not so categorized on the applicable Order, SOW or otherwise in writing, Agency Personal Data and business purposes of processing are as set forth in Attachment 1 of this DPA. Agency Personal Data may be Processed by Workiva and its Sub-processors in the United States, the UK, the EEA or other locations around the world provided that the transfer of Agency Personal Data will comply with this DPA and Applicable Data Protection Law. If Workiva reasonably believes there is a conflict with any Applicable Data Protection Law and Agency's instructions, Workiva will immediately inform Agency 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 Agency Personal Data on behalf of Agency 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 Agency (at Agency's expense) to enable Agency 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 Agency Personal Data under the Agreement. If any such request, correspondence, enquiry or complaint is made directly to Workiva, Workiva shall promptly inform Agency 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 Agency authorizes Workiva to redirect the data subject request as necessary to allow Agency to respond directly. Workiva shall provide Agency with reasonable assistance (at Agency's expense) in support of a data protection impact assessment or prior consultation with any Supervisory Authority, solely in relation to Agency Personal Data, the Services and where the Agency would not otherwise have access to the relevant information.

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

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

4.0 Transfer of Agency Personal Data.

4.1 Cross-Border Transfer. Workiva shall only transfer Agency Personal Data subject to the GDPR, UK GDPR, or FADP if it has taken necessary measures to ensure the transfer is in compliance with the Applicable Data Protection Laws and this DPA. Transfer mechanisms may include (without limitation) transferring such Agency Personal Data to a recipient: (a) in a country deemed by the European Commission, the UK Secretary of State or the UK GDPR, or the Swiss FADP as providing adequate protection for such Agency Personal Data, including a transfer pursuant to the (i) EU-US DPF and/or (ii) the UK Extension, (b) that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or (c) that has executed to the extent required the applicable standard contractual clauses adopted or approved by the European Commission, the UK Information Commissioner's Office ("**ICO**"), or the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

4.2 Data Privacy Framework**.** Workiva Inc. (Workiva's US entity) is certified under the Data Privacy Framework and where applicable, Workiva shall transfer EEA or UK Agency Personal Data to the U.S. pursuant to the EU-U.S. DPF and the UK Extension. If the DPF is no longer a legally acceptable mechanism for the transfer of EEA or UK Agency Personal Data to the U.S., the parties agree that Workiva may transfer such Agency Personal Data to the U.S. pursuant to Section 4.3, 4.4 and/or 4.6 of this DPA.

4.3 EEA SCCs. To the extent applicable, the Standard Contractual Clauses shall apply only to Agency Personal Data subject to the GDPR that is transferred to a recipient in a country not recognized by the European Commission as providing an adequate level of protection for such Agency Personal Data. The parties agree that by executing this DPA they are also

executing the Standard Contractual Clauses together with the following additional terms:

(a) Applicability. To the extent applicable, Module Two (Controller to Processor) of the Standard Contractual Clauses ("**Module Two SCCs**") shall apply where Agency and/or its Named Affiliate is a Controller and a data exporter of Agency Personal Data, and Workiva is a Processor and data importer of such Agency Personal Data. To the extent applicable, Module Three (Processor to Processer) of the Standard Contractual Clauses ("**Module Three SCCs**") shall apply where Agency and/or its Named Affiliate is a Processor and a data exporter of Agency Personal Data, and Workiva is a Processor and data importer of such Agency Personal Data. As used in this DPA, Standard Contractual Clauses or SCCs shall refer to Module Two SCCs and/or Module Three SCCs where appropriate.

(b) Instructions. This DPA and the Agreement are Agency's complete and final documented instructions at the time of signature of the Agreement or this DPA (as the case may be) for the Processing of Agency Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1(a) of Module Two SCCs and Clause 8.1(b) Module Three SCCs, the following is deemed an instruction by the Agency to Process Agency Personal Data: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing to comply with other reasonable documented instructions provided by Agency (e.g., via email) where such instructions are consistent with the terms of the Agreement and this DPA.

(c) Sub-processors. Pursuant to Clause 9 of the SCCs, Agency agrees that (i) Option 2: General Written Authorisation applies, (ii) Workiva's Sub-processors set forth in Section 7 of this DPA are authorized by Agency (or the relevant Controller), and (iii) Workiva may engage new Sub-processors as described in Section 7 of this DPA. The parties agree that sub-processing obligations pursuant to Clause 9(b) of the SCCs shall be carried out in accordance with GDPR Article 28 or applicable provisions of Applicable Data Protection Law. The parties agree that the copies of the Sub-processors agreements that must be provided pursuant to Clause 9(c) of the SCCs may have all commercial and confidential information, or clauses unrelated to the SCCs or the UK Data Transfer Addendum or their equivalent, redacted by Workiva beforehand; and, that such copies will be provided by Workiva, in a manner to be determined in its discretion, only upon written request by Agency.

(d) Audits. The parties agree that the audits described in Clause 8.9 of the SCCs shall be carried out in accordance with Section 10 of this DPA.

(e) Certification of Deletion. The parties agree that the certification of deletion of Agency Personal Data that is described in Clause 8.5 of the SCCs shall be provided by Workiva to Agency only upon Agency's request.

(f) Docking Clause. The parties agree that Clause 7 of the SCCs shall apply.

(g) Redress. The parties agree that the optional language in Clause 11 of the SCCs shall be deleted.

(h) Jurisdiction. For Clause 17 of the SCCs, the parties select Option 2 and the law of the Netherlands. For Clause 18(b) of the SCCs, the parties agree to the courts of the Netherlands.

(i) Annex 1. Annex 1 of the SCCs is as set forth in Attachment 1 of this DPA.

(j) Annex 2. For the purposes of Annex 2 of the SCCs, the description of the technical and organizational security measures are those described in Workiva's "Security Standards" (as set forth in Exhibit A to the Main Terms, and if no Exhibit A exists, as set forth here: www.workiva.com/securitystandards_3.5).

(k) Additional Terms for Module Three SCCs. Where Module Three SCCs are applicable, the parties agree to the terms of this Section. For the purposes of Clause 8.1(a), Agency hereby informs Workiva that Agency acts as a Processor under the instructions of the relevant Controller with respect of Agency Personal Data. Agency warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Workiva for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Agency shall be solely responsible for forwarding any notifications received from Workiva to the relevant Controller where appropriate. For the purposes of Clause 8.6(c) and 8.6(d), Workiva shall provide notification of a Personal Data Breach to Agency. For the purposes of Clause 8.9, all inquiries from the relevant Controller shall be provided to Workiva by Agency. If Workiva receives an inquiry directly from a Controller, it shall forward the inquiry to Agency and Agency shall be solely responsible for responding to any such inquiry from the relevant Controller where appropriate. (iv) For the purposes of Clause 10 and subject to Section 3.3 of this DPA, Workiva shall notify Agency about any request it has received directly from a data subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Agency shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

4.4 United Kingdom SCCs. To the extent applicable, the SCCs as set forth in Section 4.3 above and amended by the UK Data Transfer Addendum shall apply only to Agency Personal Data subject to the UK GDPR that is transferred to a recipient in a country not recognized by the UK Secretary of State or UK GDPR as providing an adequate level of protection for such Agency Personal Data, and where Agency and/or any Named Affiliates is a data exporter and Workiva is a data importer of

such Agency Personal Data. Where applicable, Workiva will execute the UK Data Transfer Addendum with its Sub-processors before the deadlines prescribed by the UK ICO. The parties agree that by executing this DPA they are also executing the UK Data Transfer Addendum (if applicable).

4.5 Switzerland SCCs. To the extent applicable, the SCCs as set forth in Section 4.3 above and amended in this Section 4.5 shall apply only to Agency Personal Data subject to the Swiss FADP that is transferred to a recipient in a country not recognized by the Swiss FDIC as providing an adequate level of protection for such Agency Personal Data, and where Agency and/or any Named Affiliate is a data exporter and Workiva is a data importer of such Agency Personal Data. The SCCs shall be deemed to be amended to the extent necessary to operate to provide appropriate safeguards for such transfers in accordance with the FADP, including the following:

(a) Clause 13(a) (Supervision) and Part C of Annex I are not used; the "competent supervisory authority" is the Swiss FDPIC;

(b) The term "Member State" cannot be interpreted to exclude data subjects in Switzerland from exercising their rights under the FADP;

(c) The term "Personal Data" shall be deemed to include "personal data" to the extent such personal data is protected under the FADP; and

(d) Any amendments required from time to time by the FDPIC in order to comply with the FADP, as further incorporated herein by written agreement.

Workiva is certified under the Swiss-US DPF. The parties agree that if Switzerland recognizes the adequacy of the Swiss-US DPF, Workiva and applicable Sub-processors may transfer Agency Personal Data subject to the FADP to the U.S. pursuant to the Swiss-U.S. DPF instead of the SCCs.

4.6 Alternative Transfer Mechanism. If Workiva adopts an alternative data transfer mechanism approved and authorized by the relevant EU, Swiss, or UK authorities (including any new version of or successor to the SCCs, UK Data Transfer Addendum, Binding Corporate Rules, or other framework 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 CCPA. The parties agree that Workiva is acting solely as a Service Provider with respect to Agency Personal Data subject to the CCPA. Workiva shall not, within the meaning of the CCPA, as amended, except (a) as directed or authorized by Agency, or (b) for purposes as permitted by the CCPA or by Cal. Code Reg. § 7051 (including any future revisions): (i) Sell or Share such Agency Personal Data; (ii) retain, use, or disclose Agency Personal Data for any purpose other than for the specific purpose described in Attachment 1; (iii) retain, use, or disclose Agency Personal Data for a commercial purpose other than those specified in Attachment 1; (iv) retain, use, or disclose Agency Personal Data outside of the direct business relationship between Agency and Workiva; or (v) combine Agency Personal Data with Personal Data it receives from any other source, including from data subjects themselves, except for business purposes or as otherwise permitted by the CCPA, as amended and including its implementing regulations. For the sake of clarity, such restrictions do not apply to Personal Data that has been de-identified and/or aggregated and is no longer capable of identifying an individual or Agency.

6.0 Security Controls. Workiva shall maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Agency's data and confidential and proprietary information, including Agency Personal Data, as further set forth in Workiva's "Security Standards" (as set forth in Exhibit A to the Main Terms, and if no Exhibit A exists, as set forth here: www.workiva.com/securitystandards_3.5). 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 Agency acknowledges and authorizes Workiva's use of its Sub-processors existing as of the Effective Date as set forth in Section 7.4 below. Agency 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 Agency 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 Agency with notice at least thirty (30) days in advance of engaging any new or replacement Sub-processors to Process Agency Personal Data under the Agreement ("**Sub-processor Notice**") giving the Agency 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 Agency Personal Data will be Processed. Where applicable and upon Agency'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 Agency has a reasonable belief that such new Sub-processor cannot comply with the Conditions, Agency 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, Agency 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 Agency's sole and exclusive remedy if Agency objects to any new Sub-processor. For the avoidance of doubt, Agency will be deemed to have consented to such Sub-processor absent an objection within the stated time period.

(d) Agency 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 Agency may result in delay in performing the Services, inability to perform the Services or increased fees. Workiva will notify Agency 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 Agency 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 Agency 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. A current list of Workiva's Sub-processors as may be used for Processing Agency Personal Data is available to Agency 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 Agency the updated Sub-processors list upon request by Agency.

8.0 Personal Data Breaches. After becoming aware of a Personal Data Breach Workiva will (a) notify Agency of the Personal Data Breach without undue delay; (b) investigate the Personal Data Breach; (c) provide Agency 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 Agency's handling of the matter by: (i) providing reasonable assistance with Agency's investigation; and (ii) making available relevant records, logs, files, data reporting, and other materials related to the Personal Data Breach's effects on Agency, 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 Agency 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 Agency Personal Data are subject to appropriate background check procedures as further set forth in the Security Standards. If, in the Agency'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 Agency Personal Data, Workiva will immediately terminate access by such individual and assign different and qualified individuals. Workiva will ensure that its Authorized Personnel who are engaged in the Processing of Agency 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 the Security Standards.

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 Agency Personal Data in accordance with applicable law (including the Foreign Intelligence Surveillance Act), Workiva shall: (a) inform Agency of the request to the extent permitted by applicable law so that Agency 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 Agency Personal Data.

13.0 Miscellaneous.

(a) Conflicts. In the event of any conflict or inconsistency between this DPA and the Agreement, the terms of this DPA shall prevail. In the event and to the extent of any conflict or inconsistency between the body of this DPA and the SCCs or the UK Data Transfer Addendum, the SCCs or the UK Data Transfer Addendum shall prevail.

(b) 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.

(c) 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.