This Confidential Data Privacy Agreement ("**DPA**") is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the "**Board**" or "**Jefferson County Public Schools**") and

Workiva Inc., a corporation organized under the laws of Delaware with its principal place of business located at 2900 University Ave, Ames, IA 50010 (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to the Board.

WHEREAS, the Provider and the Board recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99), applicable state privacy laws and regulations and

WHEREAS, the Provider and the Board desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, the Board and Provider agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Entire Agreement.** This DPA together with the Master Terms and Conditions attached hereto and incorporated herein is the entire agreement between the Parties and supersedes any and all agreements, representations, and negotiations, either oral or written, between the Parties before the effective date of this DPA. This DPA may not be amended or modified except in writing as provided below. This DPA is supplemented by the Board's Procurement Regulations currently in effect (hereinafter "Regulations") that are incorporated by reference into and made part of this DPA. The Regulations may be found at the following link: https://www.jefferson.kyschools.us/sites/default/files/modelprocurement.pdf. In the event of a conflict between any provision of this DPA and the Regulations, the Regulations shall prevail. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control. In the event of a conflict between the terms of this DPA and the Master Terms and Conditions, this DPA shall prevail.

2. **Term.** This DPA shall be effective as of December 14, 2022 (the "**Effective Date**") and shall continue for three (3) years, terminating on December 13, 2025.

3. **Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**"). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit "A"** (the "**Compensation**"). Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to the Board are costs associated with the compiling of Confidential Data requested under this DPA and costs associated with the electronic delivery of Confidential DATA to Provider.

4. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Confidential Data including compliance with all applicable federal, state, and local privacy laws,

rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Confidential Data.

5. **Confidential Data to Be Provided.** In order to perform the Services described above, the Board shall provide Confidential Data as identified in the Schedule of Data, attached hereto as **Exhibit "B".**

6. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Confidential Data Property of the Board.** All Confidential Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the Board. The Provider further acknowledges and agrees that all copies of such Confidential Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Confidential Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Confidential Data contemplated per the Service Agreement, shall remain the exclusive property of the Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Confidential Data, notwithstanding the above.

2. **Parent Access.** To the extent required by law the Board shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Confidential Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for the Board to respond to a parent or student, whichever is sooner) to the Board's request for Confidential Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Confidential Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Board, who will follow the necessary and proper procedures regarding the requested information.

3. **Reserved**

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Confidential Data held by the Provider pursuant to the Services, the Provider shall notify the Board in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the

Service Agreement, whereby the Subprocessors agree to protect Confidential Data in a manner no less stringent than the terms of this DPA.

6. **Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff participation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain permission from the Board's IRB prior to beginning any research or evaluation related data collection. For clarity, Provider will not be performing any services that would require Provider to undertake any of the requirements or obligations under this Article II section 6.

ARTICLE III: DUTIES OF THE BOARD

1. **Provide Data in Compliance with Applicable Laws.** The Board shall provide Confidential Data for the purposes of obtaining the Services in compliance with all federal, state, and local privacy laws, rules, and regulations applicable to the Services, all as may be amended from time to time.

2. **Annual Notification of Rights.** If the Board has a policy of disclosing Education Records and/or Confidential Data under FERPA (34 CFR § 99.31(a)(1)), the Board shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions.** The Board shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Confidential Data.

4. **Unauthorized Access Notification.** The Board shall notify Provider promptly of any known unauthorized access. The Board will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Confidential Data privacy and security, all as may be amended from time to time, including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. **Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designated Workiva Privacy as the data custodian ("Data Custodian") of the Confidential Data. The Board will release all data and information under this DPA to Data Custodian. Data Custodian shall be

responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this DPA, including confirmation of the return or destruction of data as described below. The Board may, upon request, review the records Provider is required to keep under this DPA.

3. **Authorized Use.** The Confidential Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. Provider will not contact the individuals included in the data sets without obtaining advance written authorization from the Board.

4. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Confidential Data to comply with all applicable provisions of this DPA with respect to the Confidential Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Confidential Data pursuant to the Service Agreement.

5. **Insurance.** Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of $5M. Upon request, Provider shall furnish the certificate of insurance evidencing this coverage.

6. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Confidential Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Confidential Data other than as required by this agreement, or applicable law or court order. If Provider becomes legally compelled to disclose any Confidential Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable efforts to provide the Board with prior notice before disclosure so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Confidential Data to any third party.

7. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Confidential Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Board or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive Learning purpose and for customized student Learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by the Board to return or destroy Confidential Data. Except for Subprocessors, Provider agrees not to transfer de-identified Confidential Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the Board who has provided prior written consent for such transfer. Prior to publishing any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.

8. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of or provide a mechanism for the Board to transfer Confidential Data obtained under the Service Agreement in a usable format, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the Board is received to return the data in a usable format, Provider shall dispose of all Confidential Data after providing the Board with reasonable prior notice. The duty to dispose of Confidential Data shall not extend to Confidential Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The JCPS may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the JCPS and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Confidential Data described in **Exhibit "D"**.

9. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Confidential Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to the Board. This section does not prohibit Provider from using Confidential Data (i) for adaptive Learning or customized student Learning (including generating personalized Learning recommendations); or (ii) to make product recommendations to teachers or JCPS employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Data as permitted in this DPA and its accompanying exhibits.

10. [Reserved]

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Confidential Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Confidential Data is stored.

2. **Audits.**

   a. So that the Board can verify the Provider's compliance with the DPA, upon the Board's request, the Provider shall provide to the Board (at it's the Provider'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 27001:2013: Certification; and (e) 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").
   b. If the Board reasonably demonstrates that the Reports provided are insufficient to demonstrate the Provider's compliance with the DPA or the Security Standards, at the Board's expense the Provider shall also provide written responses (on a confidential basis) to reasonable requests for information related to the Provider's processing or security of the Board's Confidential Data, including responses to information security and audit questionnaires, no more than once in any twelve (12) month period.
   c. If the Board reasonably demonstrates that the information provided pursuant to Sections 2a and 2b is insufficient to demonstrate compliance with the DPA or the Security Standards,

subject to Section 2d, the Board may perform at the Board's expense: (1) An audit in relation to the Provider's processing and security of Board Data (which may also be performed by the Board's third party auditor, subject to the Provider's reasonable approval) ("Audit"); or (2) A penetration test of an equivalent, non-production environment ("Pen Test").

d. Following receipt by the Provider of a request arising out of 2c(1) or 2c(2), the Provider and the Board 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 the Provider's business. Audits, Pen Tests and any information arising therefrom are deemed the Provider's Confidential Information. If the Board discovers any actual or potential vulnerability in connection with a Pen Test, the Board must immediately disclose it to the Provider and shall not disclose it to any third-party. The Board acknowledges that Audits and Pen Tests will be performed at the Board's own expense, with thirty (30) days advance written notice to the Provider, 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 the Provider's reasonable security and confidentiality requirements, and solely to the extent that the exercise of rights under Section 11.3 would not infringe Data Protection Laws.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Confidential Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any data security laws relating to the Services. The Provider safeguards are maintained to appropriately protect Confidential Data based on commercially reasonable and industry standard resources available to the Provider. The Provider shall implement an adequate Cybersecurity Framework based on one of the standards set forth in **Exhibit "E".** Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "E".** Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:

   a) Encrypting all data, at rest and in transit;
   b) Maintaining multi-factor authentication on accounts that can access the network or email remotely, including 3rd party accounts;
   c) Securing access to any physical areas/electronic devices where sensitive data are stored;
   d) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
   e) Ensuring all staff and 3rd parties sign a nondisclosure statement, and maintaining copies of the signed statements;
   f) Installing end-point protection including but not limited to anti-malware and anti-spyware on any device connected to the network that has access to scoped data, when applicable

4. **Applicable Data Protection Law.**

   a. General. The Provider shall provide reasonable and timely assistance to the Board (at the Board's expense) to enable the Board to respond to 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 any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the Processing of the Confidential Data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Provider, the Provider shall promptly inform Customer providing full details of the same unless otherwise prohibited. The Provider shall provide Customer with reasonable assistance (at the Board's expense) in support of a data protection impact assessment, solely in relation to Board Confidential Data, the Services and where the Board would not otherwise have access to the relevant information. Where required under the relevant Applicable Data Protection Law, the Provider shall maintain a record of all Processing activities carried out on Confidential Data on behalf of the Board in accordance with Applicable Data Protection Law.

b. Provider as a Processor. The Board and the Provider hereby agree that with respect to any Confidential Data contained in the Board Data, the Board shall be deemed to be the data controller and the contracting Provider entity shall be deemed to be the data processor as those terms are understood under Applicable Data Protection Law. Unless otherwise specifically agreed to by the Provider, Confidential Data may be Processed by the Provider and its Sub-processors in the United States provided that the transfer of Confidential Data will comply with this DPA. As between the parties, all Confidential Data Processed under the terms of the Agreement shall remain the property of the Board. To the extent such Confidential Data is not so categorized on the applicable Order or otherwise in writing, the Board's Confidential Data is limited to Users' business contact information, e.g., name, email address, phone number, and IP address. During the Agreement Term the Provider shall Process Confidential Data in accordance with the Board's written instructions (unless expressly waived in a written requirement) and as permitted in the Agreement. The Provider will act as a data processor with regard to the above mentioned Confidential Data during the Agreement Term. In the event the Provider reasonably believes there is a conflict with any Applicable Data Protection Law and the Board's instructions, the Provider will immediately inform the Board and the parties shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction.

c. Board Obligations. The Board shall ensure that its instructions comply with Applicable Data Protection Law and that the Processing of Confidential Data per the Board's instructions will not cause the Provider to be in breach of Applicable Data Protection Law. The Board is solely responsible for the accuracy, quality, and legality of (i) the Confidential Data provided to the Provider by or on behalf of the Board; (ii) how the Board acquired any such Confidential Data; and (iii) the instructions it provides to the Provider regarding the Processing of such Confidential Data. The Board represents and warrants that it has obtained all necessary consents and authorizations required under Applicable Data Protection Law to permit the Processing and international transfer of Confidential Data from Customer to the Provider.

5. **Confidential Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Confidential Data that compromises the security, confidentiality or integrity of the Confidential Data maintained by the Provider the Provider shall provide notification to the Board within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification

shall be made within a reasonable time after the incident. Provider shall follow the following process: After becoming aware of a Confidential Data Breach the Provider will (a) notify the Board of the Confidential Data Breach without undue delay; (b) investigate the Confidential Data Breach; (c) provide the Board with details about the Confidential Data Breach; and (d) make reasonable efforts to prevent a recurrence of the Confidential Data Breach. The Provider agrees to cooperate in the Board's handling of the matter by: (i) providing reasonable assistance with the Board's investigation; and (ii) making available relevant records, logs, files, data reporting, and other materials related to the Confidential Data Breach's effects on the Board, as required to comply with Applicable Data Protection Law. Confidential Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Confidential Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems. The Board shall provide notice and facts surrounding the breach to the affected students, parents or guardians, or staff, as applicable.

The Provider will maintain an incident response policy with procedures to provide the Board with reasonable assurances that the Provider can respond to any type of security event or breach, and which includes:

a. Roles and responsibilities with a team and a dedicated leader which is tested annually;
b. Methods for investigation and escalation assessing the event to determine the risk the event poses including proper escalation;
c. 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 unauthorized disclosure of or access to the Board Data (to facilitate timely notification the Board must register and maintain an up-to-date email with notice to security@workiva.com; where no such email is provided, the Board acknowledges that the means of notification shall be at the Providers's reasonable discretion);
d. 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
e. An audit of the incident conducting root cause analysis and remediation.

6. **Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.** The District agrees not to upload any Personal Information as defined by the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act").

a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

ii. A Social Security number;

iii. A taxpayer identification number that incorporates a Social Security number;

iv. A driver's license number, state identification card number or other individual identification number issued by an agency;

v. A passport number or other identification number issued by the United States government; or

vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

7. **Cloud Computing Service Providers.** If Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Provider agrees that:

Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

Pursuant to KRS 365.734(2), Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

Pursuant to KRS 365.734(2), Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

Pursuant to KRS 365.734(3), Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

ARTICLE VI: MISCELLANEOUS

8. **Termination.** Either party may terminate this DPA if the other party breaches any terms of this DPA, provided however, the breaching party shall have thirty (30) days to cure such breach and this DPA shall remain in force. The Board may terminate this DPA in whole or in part at any time by giving written notice to Provider of such termination and specifying the effective data thereof, at least thirty (30) days before the specified effective data. In accordance with **Attachment A,** the Board shall compensate Provider for Services satisfactorily performed through the effective date of termination.

9. **Destruction of Confidential Data.** Provider shall destroy all of JCPS's Confidential Data pursuant to Article IV, section 8.

10. **Priority of Agreements.** This DPA shall govern the treatment of Confidential Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence.

11. **Modification.** No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

12. **Disputes.** Any differences or disagreements arising between the Parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.

13. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or certified mail, sent to the designated representatives below.

    The designated representative for the Board for this DPA is:

    Name: Jodell Renn Title: Director of Internal Audit ___

    Address: 3332 Newburg Rd. Louisville, KY 40218

    Phone: (502)485-7745 _____ Email: Jodell.renn@jefferson.kyschools.us

    The designated representative for the Provider for this DPA is:

    Name: Workiva Privacy

    Address: 2900 University Ave, Ames, IA 50010

    Email: privacy@workiva.com

14. **Amendment and Waiver.** This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

15. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

16. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF KENTUCKY, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR JEFFERSON COUNTY KENTUCKY FOR

ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

17. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the Board no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Confidential Data within the Service Agreement. The Board has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

18. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Confidential Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Confidential Data and/or any portion thereof.

19. **Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor the Board shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

20. **Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Opportunity Clause set forth in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.

21. **Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or participate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.

22. Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.

23. **Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: _____ Date: _____
Printed Name: Dr. Marty Pollio
Title/Position: Superintendent

WORKIVIA INC.
By: DocuSigned by: Jill Klindt D69F2DF484AF4D4... Date: 11/28/2022
Printed Name: Jill Klindt
Title/Position: CFO

EXHIBIT "A"

DESCRIPTION OF SERVICES

Provider shall provide software licenses and support for the following products at prices equal or below Provider's standard pricing rates for the products:

Wdesk Government Audit Management Solution and Wdesk IT Risk and Compliance Solution & Integrated Risk Solution

COMPENSATION

Purchase orders shall be entered by each participating school. Funds for purchase shall come from individual school budgets. Total payments under this DPA shall not exceed $62,157.92 per fiscal year, running from July 1-June 30.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☐
	Other application technology meta data-Please specify:	☐
Application Use Statistics	Meta data on user interaction with application	☐
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify:	☐
Attendance	Student school (daily) attendance data	☑

WORKIVA
8.23.22 - G-DRIVE

	Student class attendance data	☑
Communications	Online communications captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☑
Demographics	Date of Birth	☐
	Place of Birth	☐
	Gender	☐
	Ethnicity or race	☐
	Language information (native, or primary language spoken by student)	☐
	Student disability information	☐

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	☐
Enrollment	Student school enrollment	☐
	Student grade level	☑
	Homeroom	☐
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☐
	Other enrollment information-Please specify:	☐

Parent/Guardian Contact Information	Address	☐
	Email	☐
	Phone	☐
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
Parent/Guardian Name	First and/or Last	☐
Schedule	Student scheduled courses	☑
	Teacher names	☑
Special Indicator	English language Learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐

Category of Data	Elements	Check if Used by Your System
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Staff Data	First and Last Name	☑
	Email Address	☑
	Staff ID number	☐
	Other information – Please specify	☐
Student Contact Information	Address	☐
	Email	☐
	Phone	☐

Student Identifiers	Local (School district) ID number	☑
	State ID number	☑
	Provider/App assigned student ID number	☐
	Student app username	☐
	Student app passwords	☐
Student Name	First and/or Last	☑
Student In App Performance	Program/application performance (typing program- student types 60 wpm, reading program-student reads below grade level)	☐
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☐
Student work	Student generated content; writing, pictures, etc.	☐

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☑
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐

	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

Compensation: Amounts to be paid to the Provider in exchange for software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider's standard pricing for that product.

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with the Board to provide a service to the Board shall be considered an "operator" for the purposes of this section.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Confidential Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Regulations: The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Confidential Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Confidential Data: Confidential Data includes any data that is uploaded by the Board or its users into Provider's Services platform, whether gathered by Provider or provided by the Board or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal

records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Confidential Data includes Meta Data. Confidential Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Confidential Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Confidential Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Confidential Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Board or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Confidential Data.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Confidential Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Confidential Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]

Signature

_____ _____

Authorized Representative of the Board Date

Verification of Disposition of Data

_____ _____

Authorized Representative of Provider Date

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	**FRAMEWORK(S)**
X	American Institute of CPAs	SOC2
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	The Board of Education of Jefferson County	Board provided standardized questionnaire

Master Terms and Conditions - USVN04042022

BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY SIGNING AN ORDER REFERENCING THESE MASTER TERMS AND CONDITIONS (INCLUDING ALL REFERENCED DOCUMENTS OR LINKS HEREIN, THE "**MASTER TERMS AND CONDITIONS**" AND ALONG WITH ALL ORDERS, THE "**AGREEMENT**") ON BEHALF OF THE COMPANY SET FORTH IN SUCH ORDER THE SIGNER IS HEREBY ENTERING INTO THE MASTER TERMS AND CONDITIONS AND THE AGREEMENT ON BEHALF OF SUCH COMPANY (THE "**CUSTOMER**") WITH THE WORKIVA ENTITY ALSO NAMED IN SUCH ORDER ("**WORKIVA**"). IN DOING SO THE SIGNER REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO BIND CUSTOMER AND ITS AFFILIATES TO THESE MASTER TERMS AND CONDITIONS AND THE AGREEMENT.

1.0 Services. Subscription Services and Professional Services (collectively referred to herein as, the "**Services**") are each available for Customer as set forth in these Master Terms and Conditions and the applicable ordering document (in the case of Subscription Services, a "**Subscription Order**," in the case of Professional Services, a "**Statement of Work**," or a "**SOW**," and for purposes of the Agreement, these ordering documents may be collectively referred to as, "Orders" or individually as, an "**Order**") entered into by Workiva and Customer.

1.1 Professional Services. Workiva shall provide professional Services such as setups, trainings, and other professional services ("**Professional Services**") as set forth in the applicable Statement of Work. Customer agrees to the Professional Services terms found at www.workiva.com/professionalserviceaddendum_1.0, which will apply to Workiva's provision of Professional Services.

1.2 Subscription Services.

(a) Pursuant to the terms of the Agreement, Workiva shall provide Customer with subscription based access, exercisable through Customer's Users (defined below), to its cloud based software programs which are made up of Workiva's proprietary software, incidental downloadable software created by Workiva, and applicable Third Party Software (as the case may be), as more adequately described in the applicable Subscription Order, and the Documentation (the "**Subscription Services**"). The Subscription Services include support as set forth in the Subscription Order ("**Support**"). "**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. "**Third Party Software**" means software and services authored by a third party, including, the Google App Engine and Amazon Web Services.

(b) 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 as applicable to any downloadable software (e.g., plug-ins)) to access, use, and display the Subscription Services. "**Users**" means employees of Customer or Affiliates (defined in Section 1.3(a)) that are provided with (or that Workiva provides at Customer's request) user identifications and passwords to Customer's account. Users may include consultants, contractors, agents, and third parties with which Customer, or a Customer Affiliate, transacts business. Users will be determined on a named user basis rather than on a concurrent user or shared user basis; provided that Customer may reassign different individuals on a reasonable basis (e.g., an employee changes positions or leaves Customer's employ). 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) Over the course of the Agreement Term Workiva may, in its sole discretion, update features, functionality, software, or user types that Customer accesses pursuant to an active Order; 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 (the "**Minimum System Requirements**"). The Minimum System Requirements are set forth in the Documentation, for Customer's reference.

1.3 Customer Affiliates.

(a) "**Affiliate**" means any corporation, partnership, joint venture, joint stock company, limited liability company, trust, estate, association, or other entity the existence of which is recognized by any governmental authority, (collectively an "**Entity**") that directly or indirectly through one or more intermediaries, controls or is controlled by or is under common control with either Customer or Workiva or any Entity in which Customer or Workiva has any direct or indirect ownership interest, whether controlling or not, of at least 50%, at any time during the Agreement Term (defined in Section 4.1 below). For purposes of this definition the term "controls", "is controlled by" or "under common control with" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities, by contract or otherwise.

(b) Except where explicitly permitted in an Order for specific Subscription Services scoped and provided pursuant to a quantifiable metric Customer may only permit Affiliates named in an Order ("**Named Affiliate**") to benefit from the Subscription Services pursuant to Customer's Agreement (in contrast to accessing the Subscription Services pursuant to such Affiliate's own Agreement). For the avoidance of doubt, any User can contribute to any given report, but reports can only be created to the benefit of the Customer or any Named Affiliate. Customer will be responsible for any Affiliate's, or any Users', compliance with the terms of the Agreement and, for purposes of the foregoing, all obligations of Customer shall apply equally to each such Named Affiliate that receives Services under a Customer Order.

2.0 Security; Customer Data.

2.1 Security. As a part of the Services Workiva shall maintain appropriate administrative, physical, and technical safeguards for the security, confidentiality and integrity of any data or information inputted, edited, authored, generated, managed, or otherwise submitted by Customer or its Users (or by Workiva at Customer's or a User's request) into Customer's subscription account ("**Customer Data**"), as described in Workiva's Security standards set forth at https://www.workiva.com/legal/securityrequirements_3.3 ("**Security Standards**"). The Security Standards shall be deemed compliant with Workiva's obligations to protect Customer Data as set forth in the Agreement. To the extent Customer Data includes personal data, Workiva represents and warrants to only process such data pursuant to Customer's requests or as otherwise set forth at www.workiva.com/dataprocessingagreement_US_1.3 (the "**Data Processing Agreement**" or "**DPA**").

2.2 Customer Data; Other Responsibilities. Workiva shall not modify, disclose (except as compelled by law in accordance with Section 5.4, or as permitted in the Agreement), or access (except to provide or improve the Services, diagnose, prevent or address service technical or performance problems, or at Customer's request in connection with Support) Customer Data. Except as otherwise agreed in writing (including as agreed in the applicable Order) and subject to Workiva's warranties set forth herein, (a) Customer is responsible for the accuracy, truthfulness, consistency, completeness, and any output from the Subscription Services, and (b) Workiva will neither have the responsibility to review, nor any liability as to the accuracy of, any information or content posted by Customer or its Users. Customer is responsible for any consents or government authorizations necessary for the collection, use and disclosure of all Customer Data in its use of the Subscription Services. The security, deletion, correction, accuracy, quality, integrity, legality, reliability, appropriateness, intellectual property ownership in, or right to use any Customer Data transmitted, exported, or sent from the Subscription Services to any third party software environment or system, shall be solely subject to the terms of Customer's agreement with such third party and Workiva will have no responsibility for Customer's use of, or Customer Data stored or residing on, such third party software environment or system and the terms of this Agreement will not apply.

2.3 Usage Data. In providing the Services, Workiva utilizes the services of Google and Amazon ("**Cloud Hosting Providers**"). Notwithstanding anything contrary in this Agreement, Workiva may collect, store and use data (other than Customer Data) relating to or derived from the operation, support, and/or about the Services, including, without limitation, information related to Customer's use of the Services and subscription account activity (the "**Usage Data**"). During and after the Agreement Term hereof, Workiva may use such Usage Data to improve and enhance the Services, for other development, diagnostic and corrective purposes in connection with the Services and Workiva's other offerings, and for purposes of operating Workiva's business. 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 (including the Cloud Hosting Providers) to collect, store and use such Usage Data, and Workiva shall be responsible for such third party service providers' compliance with the Confidentiality and other provisions of this Agreement as they relate to the collection, storage and use of Usage Data on behalf of Workiva. Workiva may not share any Usage Data with a third party except (i) as permitted in this Section 2.3, (ii) in accordance with Section 5.0 (Confidentiality) of this Agreement, or (iii) to the extent the Usage Data is aggregated and anonymized such that Customer and its Users cannot be identified.

3.0 Fees; Payment.

3.1 Invoicing. Fees for Services ("**Fees**") will be set forth in each applicable Order and Customer shall pay such Fees in advance and/or in accordance with any billing frequency or terms stated in the applicable Order. Unless otherwise specified in the applicable Order, Customer shall pay all undisputed Fees no later than thirty (30) days from receipt of invoice. If Customer has not paid all undisputed Fees in full fifteen (15) days from the invoice due date, Workiva has the right to suspend provision of Services until full payment is paid by Customer, provided that Workiva has given Customer notice of such overdue Fees. Workiva will provide written notice of an Order's renewal at least forty-five (45) days prior to the expiration thereof, which may include an increase to Customer's Fees for such renewal.

3.2 Disputes. If Customer disputes any Fees invoiced, Customer may provide Workiva written notice of such dispute within fifteen (15) days from receipt of the applicable invoice; failure to do so will forfeit Customer's right to withhold payment or dispute such Fees. Customer and Workiva will then work in good faith to attempt to resolve such contested amounts, provided, however, that Customer will remain responsible for the portion of Fees that are not disputed. Upon the parties' resolution of any dispute over Fees, Customer shall pay such Fees found to be due and owing as soon as reasonably practicable.

3.3 Metric Compliance. Fees for Subscription Services will be pursuant to the terms of, and the metrics defined in, a Subscription Order. Workiva reserves the right to verify Customer's compliance with Subscription Order metric(s). To the extent that Customer exceeds any such metric, Workiva will provide written notice to Customer regarding such exceeded metric and give Customer an opportunity to cease exceeding such metric no later than thirty (30) days after Workiva's delivery of notice. If Customer has not ceased exceeding the applicable metric within

such thirty (30) day period Workiva may charge Customer additional Fees, at Workiva's then current rates, based on the metric defined in the applicable active Subscription Order that continues to be exceeded. If the Customer's usage of the Service(s) continues to be in excess of the licensed metric defined in the active Subscription Order, then upon Workiva's request, Customer shall execute documentation memorializing the change to the scope of the Subscription Services and related Fees based on the applicable active Subscription Order metric(s). In the absence of a new Order, Customer will remain responsible for all fees associated with the exceeded metric. Workiva may not unilaterally add additional, modify or remove existing, metrics once an Order is signed.

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 as Workiva may 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; Payment Processors. To the extent Customer requires the use of a purchase order (or Customer's requirement that a party complete other administrative steps) prior to making any payments under the Agreement, Customer acknowledges that doing so is solely for Customer's administrative convenience, and accordingly Customer's failure to submit such purchase order to Workiva (or a party's completion of other administrative steps) does not excuse Customer from payment of the Fees in the amounts, or in the manner, agreed upon herein or in the applicable 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 or related nature. 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.

4.0 Term; Termination.

4.1 Agreement Term. The Agreement begins on the Start Date of the first Order between the parties hereto, and shall continue until all Subscription Orders associated with the Agreement have expired or been terminated (the "**Agreement Term**"), subject to Section 10.9.

4.2 Subscription Term. The Subscription Services will begin on the Start Date in the applicable 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 4.2.

4.3 Statements of Work Terms. The period of performance set forth in SOWs for Professional Services will be as agreed upon by the parties and set forth in the applicable SOW.

4.4 Termination for Convenience. Customer may terminate the Agreement or an Order without cause upon thirty (30) days written notice. If Customer terminates without cause, Customer will remain responsible for all Subscription Services Fees set forth in the applicable Order(s), but Workiva will refund any prepaid and unearned Fees for Professional Services outstanding as of the effective date of termination. Regardless of Customer's exercise of its rights under this Section 4.4 any unpaid Fees for the then current Subscription Term (e.g., fixed and agreed upon amounts that are billed in annual installments) 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. Workiva may terminate an Order without cause upon ninety (90) days written notice, provided that it shall refund all unearned Fees within thirty (30) days of the termination effective date.

4.5 Termination for Material Breach. 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. The non-breaching party may elect to terminate the applicable Order only or the Agreement as a whole (and thus, all Orders hereunder). In the event the Agreement is terminated due to Workiva's uncured material breach, Workiva will refund all unearned Fees within thirty (30) days of the termination effective date.

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

4.7 Survival. Neither expiration nor termination of the Agreement will terminate those obligations and rights of the parties pursuant to provisions of the Agreement 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 4.7, 5, 6, 7, 9, and 10 of these Master Terms and Conditions will survive the expiration or termination of the Agreement regardless of when such termination becomes effective.

5.0 Confidentiality.

5.1 Confidential Information. In connection with the Agreement, each of the parties may disclose to the other party information that relates to the disclosing party's or disclosing party's customers' business operations, financial condition, customers, products, services, or technical knowledge ("**Confidential Information**"). Except as otherwise specifically agreed in writing, each party agrees that: (a) all information communicated to it by the other 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, and (c) all information communicated to it that reasonably should have been understood by the receiving party, because of confidentiality, descriptions or similar legends, the circumstances of disclosure or the nature of the information itself, to be confidential to the disclosing party, will be Confidential Information and will be deemed to have been received in confidence and will be used only for purposes of the Agreement. "Confidential Information" includes the information exchanged between the parties related to future business relationships or Services not currently addressed under the Agreement, including but not limited to requests for proposals, bids, correspondence, negotiations, and discussions. Any non-disclosure agreement entered into by the parties after the Effective Date shall be of no force or effect unless such non-disclosure agreement by its terms expressly supplements, modifies, or replaces this Section 5 of these Master Terms and Conditions. Workiva Confidential Information includes the Subscription Services, Services, Fees, the terms of the Agreement, development plans, and any security specifications, reports or assessments related to the Subscription Services, Workiva or its Cloud Hosting Providers. Customer Confidential Information includes Customer Data.

5.2 Standard of Care; Third Parties. Each party will use at least the same degree of care to safeguard and to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure or publication of its own information (or information of its customers) of a similar nature, and in any event, no less than reasonable care. Each party may disclose relevant aspects of the other party's Confidential Information to its employees to the extent such disclosure is reasonably necessary for the performance of its obligations, or the enforcement of its rights, under the Agreement; provided, however, that such party will use reasonable efforts to ensure that all such persons comply with these confidentiality provisions. Each party may disclose the other party's Confidential Information to third parties provided that such third parties are 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. These third parties are restricted to using the Confidential Information for the sole purpose of providing the contracted services to the party. Each party will be responsible for any improper disclosure of Confidential Information by such party's employees, agents, or contractors.

5.3 Preclusion on Use. 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 the 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 the Agreement) to promptly return to the other party its Confidential Information (including copies thereof) if requested to do so. Upon expiration or termination of the Agreement and completion of a party's obligations under the Agreement, each party will return or destroy, as the other party may direct, the other party's Confidential Information, and retain no copies. Workiva may 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 obtain Customer Data. 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.

5.4 Exclusions; Permitted Use. This Section 5 will not apply to any particular information that either party can demonstrate (a) was, at the time of disclosure to it, in the public domain, (b) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party, (c) was in the possession of the receiving party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation, (d) was received after disclosure to it from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations) to it, 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 5 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, and 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.

5.5 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 by any person that may become 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.

5.6 Log-Ins and Passwords. In addition to the foregoing obligations, Customer agrees to hold the Subscription Services and all associated log-ins and passwords in confidence, and to protect the confidential nature thereof, and shall not disclose any trade secrets contained, embodied, or utilized therein, to anyone other than a User having a need for such disclosure, and then only to allow use of the Subscription Services as authorized herein. Customer shall take all reasonable steps to ensure that the provisions of this Section 5.6 are not violated by any employee, User, or any other person under Customer's control or in its service.

6.0 Ownership; Usage Restrictions.

6.1 Workiva Ownership. Workiva (or its licensors, as the case may be) 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. Customer acknowledges and agrees that Workiva (or its licensors, as the case may be) shall own all right, title and interest in and to any modifications, derivative works, changes, expansions or improvements to the Services, without any other or subordinate right whatsoever being held by Customer. Customer shall acquire no rights therein other than those limited rights of use specifically conferred by the Agreement. Customer may not create derivative works based upon the Services in whole or in part, or develop or request third parties to develop or modify any software based on ideas, processes, or materials incorporated therein. Customer shall not 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. All rights related to the Services that are not expressly granted to Customer under the Agreement are reserved by Workiva (or its licensors, as the case may be). In the event that Customer or its Users provides Workiva with any comments, suggestions, or other feedback with respect to the Services (**"Feedback"**), Customer hereby grants Workiva a perpetual, irrevocable, royalty-free, fully paid-up, worldwide license to use any such Feedback, and Workiva has the right, but not the obligation, to use such Feedback in any way without restriction or obligation to Customer. Workiva will be free to use for any purpose, any ideas, concepts, know-how, or techniques that result from such Feedback, and Workiva will be the exclusive owner of any modifications, enhancements, or derivative works of the Services resulting from Workiva's use of such Feedback. Upon Workiva's reasonable request, Customer agrees to execute such additional documents if necessary for perfecting or recording Workiva's ownership interest, provided that preparation of such additional documents shall be at the expense of Workiva.

6.2 Customer Ownership. As between Workiva and Customer, Customer is, and will remain, the owner of all Customer Data. With the exception of a limited license granted to Workiva to use Customer Data for the purpose of performing the Services, in accordance with Section 2, 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. Any reports or documents generated through Customer's use of the Subscription Services in accordance with this Agreement will be owned by Customer. If such reports or documents include any pre-existing intellectual property owned by Workiva, Workiva hereby grants to Customer a 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 Customer's reports or documents.

6.3 Artificial Users. Workiva hereby permits Customer's use of "bots", artificial intelligence, computer scripts, robotic process automation, or similar type of non-human Users (**"Artificial Users"**) subject to the following:

(a) To the extent Artificial Users disrupt the integrity or performance of the Services, Subscription Services, or any data of Workiva's other customers, or infringes, or allegedly infringes, the intellectual property rights of a third party, Customer will be in material breach of the Agreement and Workiva reserves the right to immediately suspend such Artificial Users or Services as a whole. Workiva will provide Customer with subsequent notice regarding such suspension and/or material breach. To the extent Workiva is unable to suspend such Artificial Users in accordance with the foregoing, Customer agrees to immediately, upon Workiva's request, discontinue use of, and/or suspend such Artificial Users.

(b) Customer hereby warrants (i) that it is the owner (or valid licensee) of and retains all title to, and all intellectual property rights in, the Artificial Users, and (ii) that introducing the Artificial Users into the Subscription Services will not violate or infringe the rights of any third party.

(c) Customer acknowledges and agrees that its use of Artificial Users does not preclude Workiva from developing similar technology. In addition Workiva will have an unlimited license to use any ideas, concepts, know-how or techniques that result from any discussions regarding the use of Artificial Users, including modifications or enhancements to the Services or Subscription Services.

(d) WORKIVA DOES NOT WARRANT THAT THE ARTIFICIAL USERS WILL ACHIEVE CUSTOMER'S EXPECTED RESULTS OR OTHERWISE OPERATE WITHOUT FAULT OR ERROR IN CONJUNCTION WITH THE SUBSCRIPTION SERVICES, SERVICES, SUPPORTING SYSTEMS, OR ANY MODIFICATIONS OR UPDATES THERETO AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, WORKIVA AND ITS LICENSORS HEREBY EXPRESSLY DISCLAIMS ANY SUCH WARRANTY. If a malfunction of the Subscription Services is due to a problem with Artificial Users Workiva will so inform Customer and, notwithstanding anything in the Agreement, it will be Customer's responsibility to (i) provide reasonable information and support to assist Workiva in its efforts to address any malfunctions of the Subscription Services, caused, or allegedly caused, by the Artificial Users, or (ii) obtain and/or pay for any repairs or modifications required to ensure proper functioning of such Artificial Users.

6.4 Subscription Usage Restrictions. Customer and its Users may access and use the Subscription Services (a) for Customer's or Named Affiliate's business use only, (b) solely as set forth, and subject to any restrictions, in the Agreement (including, without limitation, product descriptions shown in the Subscription Order), and (c) not for the benefit of, or to provide services to, any third party (including, without limitation, Affiliates that are not Named Affiliates). Customer shall not grant rights of access to the Subscription Services to anyone other than Users without Workiva's prior written consent. The rights granted to Customer under the Agreement may not be sold, resold, assigned (except as set forth in Sections 1 and 10), leased, rented, sublicensed, or otherwise transferred or made available for use by third parties, in whole or in part, by Customer without Workiva's prior written consent. For the avoidance of doubt, Customer may allow an Affiliate to use the Subscription Services under Customer's Order for such Affiliate's benefit, subject to Section 1. Customer shall not 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 the Agreement, or facilitate any such unauthorized access for any third party. If any unauthorized access occurs, Customer shall promptly notify Workiva of the incident and shall reasonably cooperate in resolving the issue. Customer shall not reverse engineer, decompile, or disassemble any Subscription Services or otherwise attempt to discover the source code thereof or permit any third party to do so. Customer shall not attempt to disable or circumvent any security measures in place. Customer may not knowingly reproduce or copy the Subscription Services, in whole or in part. Customer shall not modify, adapt, or create derivative works of the Subscription Services. Customer shall not 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. Customer shall not knowingly interfere with or disrupt the integrity or performance of the Subscription Services or third party data contained therein.

7.0 Warranties; Disclaimers.

7.1 Mutual Representations and Warranties. Each party represents and warrants to the other party that: (a) it is duly organized, validly existing, and in good standing as a corporation or other entity under the laws of the jurisdiction of its incorporation or other organization, (b) it has, and throughout the Agreement Term, will retain, the full right, power, and authority to enter into the Agreement and perform its obligations hereunder, (c) the execution of any of the documents that comprise the Agreement by its representative has been duly authorized by all necessary corporate or organizational action of such party, (d) when executed and delivered by both parties, an Order incorporating these Master Terms and Conditions will constitute the legal, valid, and binding obligation of such party, enforceable against such party in accordance with its terms, and (e) in exercising its rights and performing its obligations as set forth in this Agreement, each party will comply with the laws applicable to such party's business.

7.2 Workiva Representations and Warranties. Workiva warrants (a) that the Subscription Services will perform materially in accordance with the Documentation and the Agreement, (b) to use best efforts to correct material defects that are reported by Customer or its Users and otherwise provide the Subscriptions Services as further set forth in the service levels in the applicable Order (if a malfunction is due to a problem with Customer hardware or software, Workiva will so inform Customer and it will be Customer's responsibility to obtain and pay for any repairs or modifications required for such Customer hardware or software), (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 the 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 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 Customer Acknowledgments. Customer accepts responsibility for selection of the Services to achieve Customer's intended results. Customer is solely responsible for obtaining all necessary rights and consents to enter Customer Data into the Subscription Services and hereby represents and warrants that Customer has sufficient rights in and in providing Customer Data to Workiva under the Agreement 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. The parties do not intend Customer to use the Subscription Services that would create obligations under The Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Gramm-Leach-Bliley Act ("**GLBA**") or similar laws and Workiva makes no representations that the Subscription Services satisfy the requirements of such laws. If Customer is (or becomes) a Covered Entity or Business Associate (as defined in HIPAA) or a Financial Institution (as defined in GLBA), Customer agrees not to use the Subscription Services to store or process unmasked Protected Health Information (as defined in HIPAA) or Nonpublic Personal Information (as defined in GLBA). Accordingly, Customer represents that its use of the Services does not require Workiva to execute a business associate agreement, to enter into any other agreement with Customer, or create other obligations under HIPAA.

7.4 Disclaimers. 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. Workiva does not warrant that the Subscription 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. Customer acknowledges and agrees that Workiva and its licensors are not responsible for: (i) the accuracy or integrity of any Customer Data, (ii) the performance of Customer's or its Users' equipment, hardware, Artificial Users, or software, (iii) delivery of services or connectivity provided by third parties to Customer and its Users, or (iv) any loss or corruption of Customer Data that occurs as a result of transmitting or receiving Customer Data or viruses due to Customer's, or its Users', connection and access to the internet.

8.0 Infringement Indemnification.

8.1 Obligation to Defend. 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 damages and costs finally awarded or agreed to in settlement by Workiva (including reasonable attorneys' fees).

8.2 Procedures for Indemnification. Workiva's obligations under Section 8.1 are expressly conditioned on the following: Customer shall (a) promptly notify Workiva in writing of any such claim of which Customer has actual knowledge (provided that failure to do so will only release Workiva from this obligation to the extent that such failure led to material prejudice), (b) in writing, grant Workiva 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 Customer, and (c) reasonably cooperate with Workiva to facilitate the settlement or defense of the claim.

8.3 Replacement Software. Should the Subscription Services become, or of in Workiva's opinion is 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 function is performed by the replacement or modified Subscription Services, or (c) if in Workiva's judgment the right to continue to use the Subscription Services cannot be reasonably procured or the Subscription Services cannot reasonably be replaced or modified, 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.

8.4 Combination. Workiva shall have no obligation under the foregoing with respect to: (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) any claim for which Customer is obligated under Section 6.3 or 6.4, or (c) any claim which would not have occurred but for Customer's modification.

8.5 Limitation. This Section 8 states the entire liability of Workiva with respect to third party infringement arising from the Services, or any parts thereof, and Workiva shall have no additional liability with respect to any alleged or proven infringement.

9.0 Limitation of Liability and Disclaimers of Damage.

9.1 Limit on Liability. Subject to Section 9.2, for all claims by either party against the other party, whether such claims are made in contract, tort, strict liability, or otherwise shall be limited to the actual, direct damages suffered by such party up to: (a) the actual amount paid or payable by Customer to Workiva under this Agreement during the twelve (12) months prior to such claim(s) for the specific Service(s) giving rise to such claim(s), and (b) with respect to Workiva's breaches of its obligations under Section 5.0 (Confidentiality), the Security Standards, and the DPA, an amount equal to two times (2x) the actual amount paid by Customer to Workiva under this Agreement during the twelve (12) months prior to such claim(s) for the specific Service(s) giving rise to such claim(s) (the "**Enhanced Cap**").

9.2 Exclusions to the Limitation on Liability. The limitations in Section 9.1 shall not apply to: (a) the indemnity obligations set forth in Section 8, (b) either party's gross negligence, fraud, criminal acts or willful misconduct, (c) Customer's payment obligations, (d) liability arising out of Customer's obligations under Section 6.3, and (e) Workiva's liability under Section 9.3 below.

9.3 Workiva Liability for Personal Data Breaches. In the event of a Personal Data Breach that is the direct result of the failure of Workiva to comply with the terms of this Agreement, Workiva shall bear the actual, reasonable costs of notifying affected individuals and providing one (1) year of commercially reasonable credit monitoring to individuals in jurisdictions where monitoring is available. Workiva and Customer shall mutually agree on the content and timing of any such notifications, in good faith and as needed to meet applicable legal requirements. Notwithstanding the preceding sentence, the parties agree that Workiva shall have no obligation to send notification letters or provide credit monitoring for Customer unless such letters are legally required or otherwise reasonably required to alert individuals of potential harm.

9.4 DISCLAIMER OF CERTAIN DAMAGES. TO THE FULLEST EXTENT PERMITTED BY LAW, (A) IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY LOSSES 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

AND (B) IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY LOSS OF REVENUES, LOSS OF PROFITS, LOSS OF BUSINESS, OR LOSS OF DATA, ARISING (WHETHER DIRECTLY OR INDIRECTLY) OUT OF CUSTOMER'S FAILURE TO USE THE SUBSCRIPTION SERVICES IN ACCORDANCE WITH THE DOCUMENTATION. THE FOREGOING EXCLUSION SHALL NOT APPLY TO CLAIMS FOR CONSEQUENTIAL DAMAGES ARISING FROM WORKIVA'S OR CUSTOMER'S (I) GROSS NEGLIGENCE, FRAUD, CRIMINAL ACTS OR WILLFUL MISCONDUCT, (II) DEATH OR PERSONAL INJURY CAUSED BY WORKIVA'S OR CUSTOMER'S NEGLIGENCE OR (III) BREACH OF SECTION 5 UNDER THIS AGREEMENT; PROVIDED, HOWEVER, THAT ANY CONSEQUENTIAL DAMAGES RECOVERED BY CUSTOMER OR WORKIVA FOR CLAIMS PURSUANT TO SECTION 5 WILL BE SUBJECT TO THE ENHANCED CAP. FURTHER, ANY CLAIM AS A RESULT OF A BREACH OF SECTION 2, THE SECURITY STANDARDS, OR THE DPA, SHALL NOT BE DEEMED A BREACH OF SECTION 5, AND ACCORDINGLY, SHALL BE SUBJECT TO THE DISCLAIMERS IN THIS SECTION 9.4.

10.0 Miscellaneous.

10.1 Public Announcements. Unless otherwise agreed by the parties in an Order, Customer grants Workiva the right to use Customer's name, logo, trademarks, quotes, and/or trade names in press releases, product brochures, sales presentations, financial reports, webinars, and on its websites indicating that Customer is a customer of Workiva. All other public statements or releases require the mutual consent of the parties.

10.2 Non-Solicitation. Each party recognizes that the other party's employees constitute valuable assets. Accordingly, neither party will, during the Agreement Term and for a period of one (1) year thereafter, directly solicit any of the other's employees for positions of employment or as consultants or independent contractors. Notwithstanding the foregoing, neither party is precluded from (a) hiring an employee of a party that independently approaches it, (b) indirectly soliciting the other party's employees through the use of a staffing agency, provided that the party has not provided the staffing agency with names or other information to facilitate the solicitation of the other party's employee or contractor, or (c) conducting general recruiting activities, such as participation in job fairs or publishing advertisement in publications or on websites for general circulation.

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 hand, confirmed electronic transmission, or nationally recognized overnight courier, or five (5) days after being sent by certified or registered mail, postage and charges prepaid, return receipt requested, to the address, facsimile number, or the 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; Jurisdiction. Without regard to its conflicts of laws principles, the laws of Delaware govern all matters arising under or relating to the Agreement. Any and all actions, suits, or judicial proceedings upon any claim arising from or relating to this Agreement shall be instituted and maintained in the State of Iowa. If it is judicially determined that either party may file an action, suit, or judicial proceeding in federal court, such action, suit, or judicial proceeding shall be in the Federal District Court for the Southern District of Iowa.

10.6 Assignment. Neither party may assign the 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 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 by 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 the Agreement.

10.8 Injunctive Relief. Each party acknowledges and agrees that a breach, including an anticipatory or threatened breach, by either party of any of its obligations under Sections 5 or 6 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 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. Workiva Inc., its Affiliates and licensors, as well as Customer's Affiliates that receive access as set forth in Section 1, may be third party beneficiaries of the Agreement. No other third party, including without limitation Customer's addition of third party Users, is intended to be a beneficiary of the Agreement entitled to enforce its terms directly. As of the start date in Customer's initial Subscription Order unless otherwise stated therein there are no terms and conditions for Third Party Software with which Customer must comply. If after Workiva commences its provision of Subscription Services any underlying Third Party Software becomes subject to additional terms and conditions, upon reasonable prior written notice to Customer such terms may be attached to the Agreement, or otherwise incorporated by reference. If Customer does not consent to such terms it must notify Workiva of its rejection within thirty (30) days of receipt of such notice and, notwithstanding anything to the contrary in Section 4.1 of these Master Terms and Conditions, the Agreement will continue under the terms and conditions previously in place until the completion of all then active Subscription Terms, at which time the Agreement and all Orders hereto will expire and be of no further force or effect. 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 Federal Government End Use Provisions. Workiva provides the Services, including related software and technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Subscription Services include only those rights customarily provided to the public as defined in these Master Terms and Conditions. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data-Commercial Items) and DFAR 227.7202-03 (Rights in Commercial Computer Software or Computer Software Documentation). If any portion of the Subscription Services is deemed "non-commercial," the Services are licensed under the terms hereof and under the RESTRICTED RIGHTS set forth in the applicable FARs and DFARs (and the government's use, duplication and disclosure rights are restricted as set forth therein). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Workiva to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

10.11 Pre-Release Data. The Parties acknowledge that Customer Data may include Customer material non-public information (the **"Pre-Release Data"**) and that various laws may impose certain restrictions on trading securities of an issuer when in possession of Pre-Release Data and on communicating such information to any other person under circumstances in which it is reasonably foreseeable that such person is likely to trade in such securities based on such Pre-Release Data. 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.

10.12 Export and Import Controls and Economic Sanctions. The Services may be subject to the export and import laws of the United States and other countries. Customer agrees to comply with all applicable export and import laws and regulations. Customer acknowledges that the Services may not be exported or re-exported to any U.S. embargoed countries or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Persons List or Entity List. 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 located in any such country or on any such list. Customer agrees that Customer 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. Customer acknowledges that 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.

10.13 Electronic Storage. The parties intend to allow for the electronic imaging and storage of the Agreement, and the admissibility into evidence of such an image in lieu of the original paper version of the Agreement. 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.

10.14 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 of these Master Terms and Conditions, and constitutes the entire Agreement between the parties. 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. No oral statements or material not specifically incorporated herein will be of any force and effect. With the exception of (a) modifications to the Documentation (which may not be unilaterally modified by Workiva except to ensure compliance with Section 7.2), (b) other URLs referenced in these Master Terms and Conditions or an Order (which may not be unilaterally modified by Workiva in a manner that would be detrimental to Customer in Customer's reasonable discretion), (c) any terms or conditions associated with additional Services available for purchase, or otherwise, via Workiva's website that have been accepted or acknowledged (electronically or otherwise) by Customer or a User, and (d) as mutually agreed in an Order, no changes in or additions to these Master Terms and Conditions will be recognized unless incorporated herein by amendment and signed by duly

authorized representatives of both parties. With the exception of the Documentation, in the event Workiva updates a URL in accordance with the foregoing, and Customer determines such modification is detrimental to Customer, it shall so inform Workiva and Workiva will remain bound by the URL(s) previously agreed upon. For the avoidance of doubt, factual updates to the Documentation may not be voided by Customer in accordance with the foregoing. The application of Customer's general terms and conditions in any general vendor acknowledgement or Customer's other general purchasing conditions are hereby expressly excluded and objected to by Workiva. These Master Terms and Conditions shall apply and supersede the pre-printed terms and conditions of any form submitted, in electronic format or otherwise, by either party. The Agreement will not be construed against either party as the purported drafter. 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. In the event 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 Master Terms and Conditions shall not be used to interpret or construe its provisions. The following order of precedence will be followed in resolving any inconsistencies between the terms of these Master Terms and Conditions and the terms of any Orders, exhibits, statements of work, or other documents: first, the Sections 1 - 10 of these Master Terms and Conditions, including any referenced URLs (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.

USVN04042022

Newsroom

News

Press Releases

Select Region

Cookie Preferences

Legal

Privacy Policy

Sitemap

2900 University Blvd
Ames, IA 50010

AICPA SOC

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY): 08/03/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Aon Risk Services Central, Inc. Omaha NE Office 17807 Burke Street Suite 401 Omaha NE 68118 USA	PHONE (A/C. No. Ext): (402) 697-1400	FAX (A/C. No.): (402) 697-0017
	E-MAIL ADDRESS:	

INSURED	INSURER(S) AFFORDING COVERAGE		NAIC #
Workiva Inc. 2900 University Blvd. Ames IA 500108665 USA	INSURER A:	Great Northern Insurance Co.	20303
	INSURER B:	Chubb Indemnity Insurance Co.	12777
	INSURER C:	Federal Insurance Company	20281
	INSURER D:	Columbia Casualty Company	31127
	INSURER E:	Ascot Insurance Company	23752
	INSURER F:	Endurance American Insurance Company	10641

Holder Identifier :

COVERAGES **CERTIFICATE NUMBER:** 570094785187 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY			36057207	07/31/2022	07/31/2023	EACH OCCURRENCE	$1,000,000
	CLAIMS-MADE X OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$1,000,000
							MED EXP (Any one person)	$15,000
							PERSONAL & ADV INJURY	$1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$2,000,000
	X POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$2,000,000
	OTHER:							
A	AUTOMOBILE LIABILITY			7362-26-02	07/31/2022	07/31/2023	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
	X ANY AUTO						BODILY INJURY (Per person)	
	OWNED AUTOS ONLY / HIRED AUTOS ONLY / SCHEDULED AUTOS / NON-OWNED AUTOS ONLY						BODILY INJURY (Per accident)	
							PROPERTY DAMAGE (Per accident)	
C	X UMBRELLA LIAB X OCCUR			78192185	07/31/2022	07/31/2023	EACH OCCURRENCE	$10,000,000
	EXCESS LIAB CLAIMS-MADE						AGGREGATE	$10,000,000
	DED RETENTION							
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N			71776720	07/31/2022	07/31/2023	X PER STATUTE OTH-ER	
	ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? N (Mandatory in NH)	N/A					E.L. EACH ACCIDENT	$1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE-EA EMPLOYEE	$1,000,000
							E.L. DISEASE-POLICY LIMIT	$1,000,000
D	Cyber Liability			596697975 Tech-Cyber E&O SIR applies per policy terms & conditions	07/31/2022	07/31/2023	Tech E&O Agg Lmt SIR	$10,000,000 $500,000

Certificate No : 570094785187

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Evidence of Coverage.
A Waiver of Subrogation is granted in favor of Certificate Holder in accordance with the policy provisions of the Workers Compensation and Professional liability policies. Should any of the above described policies be cancelled before the expiration date thereof, the policy provisions will govern how notice of cancellation may be delivered to certificate holders in accordance with the policy provisions of each policy.

CERTIFICATE HOLDER

Workiva Inc.
2900 University Blvd.
Ames IA 500108665 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services Central Inc.

AGENCY CUSTOMER ID: 570000067027
LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services Central, Inc.	Workiva Inc.
POLICY NUMBER: See Certificate Number: 570094785187	
CARRIER: See Certificate Number: 570094785187 / NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER	
INSURER	
INSURER	
INSURER	

ADDITIONAL POLICIES If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS	
	OTHER							
F	E&O Tech-XS			PRX30001807202 Tech E&O XS $5M p/o $10M	07/31/2022	07/31/2023	Tech E&O Excess Lmt	$10,000,000
E				EOXS221000086002 Tech E&O XS $5M p/o $10M	07/31/2022	07/31/2023		