State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT WITH QUALTRICS, LLC.

This State of Oklahoma Contract ("Contract") is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Qualtrics, LLC ("Supplier") pursuant to 62 O.S. §34.11.1 and in connection with Oklahoma Statewide Contract # 1056 and is effective as of the date of last signature to this Contract. The term of this Contract is for one (1) year and there are four (4) one-year options to renew the Contract which the parties may exercise via signed, written agreement.

Purpose

The State is awarding this Contract to Supplier for the provision of Survey Tools as more particularly described in certain Contract Documents attached herein. This Contract memorializes the agreement of the parties with respect to the terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.

2. The following Contract Documents are attached hereto and incorporated herein:

    2.1. General Terms, Attachment B;
    2.2. Statewide 1056-Specific Terms, Attachment C;
    2.3. Information Technology terms, Attachment D;
    2.4. Portions of the Bid, Attachment E;
        i. Attach E, Ex-1 Qualtrics LLC's General T&Cs for Cloud Services;
        ii. Attach E, Ex-2 Qualtrics Public Sector Addendum to General T&Cs; and
        iii. Attach E, Ex-3 Qualtrics LLC Pricing.

For clarity, Attachments A; D, Ex-1; and F have been intentionally omitted.

3. The parties additionally agree:

3.1. except for any information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

By: D. Jerry Moore

Name: D. Jerry Moore

Title: Chief Information Officer

Date: Oct 5, 2022

QUALTRICS LLC

By: Mark Creer

Name: Mark Creer

Title: Director

Date: Oct 5, 2022

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 Except for Customer's use of the Cloud Services in excess of the Usage Metrics, at no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, except for Customer's use of the Cloud Services in excess of the Usage Metrics, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 Upon expiration of each term, the Cloud Service may be renewed for a successive one-year term with a price increase of no more than 3% at such renewal via a negotiated, signed agreement by the parties. If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by

Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request

2 Contract Effectiveness and Order of Priority

2.1 Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2 Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

A. any Addendum;

B. any Contract-specific terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

C. the terms contained in this Contract Document;

D. Intentionally Omitted;

E. any statement of work, work order, or other similar ordering document as applicable; and

F. other mutually agreed Contract Documents.

2.3 If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract Document. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by

electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract Documents

3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by either party, is not valid. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the party which made such change shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Addendum** means a mutually executed, written modification to a Contract Document.

4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.

4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering

document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.

4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

4.11 **Indemnified Parties** means the Customer and its officers, directors, agents, and employees.

4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

4.14 **OAC** means the Oklahoma Administrative Code.

4.15 **OMES** means the Office of Management and Enterprise Services.

4.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.18 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

4.19 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act. For clarity, Supplier Confidential Information includes: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5 of the General Terms and Conditions, (ii) information regarding Supplier research and development, product offerings, and availability, and (iii) subject to the prior sentence, any information which Supplier protects against unrestricted disclosure to others that (a) Supplier or its representatives designates as confidential at the time of disclosure, or (b) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure, which may include Supplier trade secrets and information relating to the security of the Cloud Service.

4.21 **Intentionally Omitted**.

5 Pricing

5.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed. Customer and Supplier are under mutual understanding that any license under this agreement is with a state agency that is exempt from sales and use tax. In the event it is determined sales and use tax is owed, Supplier will bear any applicable sales and use taxes, interest, and penalties.

5.2 Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3 Where applicable, the price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

6.1 Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2 Services will be performed in substantial conformance with the Documentation and in accordance with industry standard practices expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service. Unless otherwise required by applicable law or otherwise provided under the Contract, Customer's sole and exclusive remedies and Supplier's entire liability for breach of the foregoing will be (a) the re-performance of the deficient Cloud Service, and (b) if Supplier fails to re-perform, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three months of Supplier's failure to re-perform

6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document.

7 Invoices and Payment

7.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B.

The following terms additionally apply:

A. An invoice shall contain the purchase order number (if provided by Customer), description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2 as meaning any invoice which is complete in all requirements for processing for payment in accordance with the terms of appropriate contracts or purchase orders and applicable State or Federal statutes, including but not limited to such documentation as may be required.

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. Intentionally Omitted.

E. Customer cannot withhold, reduce or set-off fees owed during the Subscription Term.

F. Intentionally Omitted.

G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H. The Supplier shall accept payment (up to $12,500.00 per invoice) by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of (in the form of a blanket certificate of insurance evidencing existence of the required coverage), insurance coverage with the applicable liability limits set forth below. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. The minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation in compliance with statutory requirements and Employer's Liability Insurance with limits of $1,000,000 each accident, $1,000,000 by disease each employee and $1,000,000 by disease policy limit;

B. Commercial General Liability Insurance with a limit of $1,000,000 per occurrence and in general aggregate;

C. Commercial Automobile Liability Insurance with a combined single limit of $1,000,000 per occurrence;

D. Intentionally Omitted;

E. Technology professional liability with a limit of $5,000,000 per claim and in the aggregate covering claims arising out of errors or omissions in connection with services provided by Supplier as described in the Agreement and including network security and private data risks involving unauthorized access, failure of security, transmission of malicious code, denial of service attacks, and unauthorized disclosure or misappropriation of private data. The policy shall have a retroactive date on or before the Agreement effective date or the date of Supplier's first professional service, whichever is earlier.; and

F. Excess\umbrella liability with a limit of $5,000,000 per occurrence and in the aggregate with respect to coverage required in (B) and (C).

8.2 Intentionally Omitted.

8.3 Intentionally Omitted.

9 Compliance with Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C. Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Applicable federal immigration laws and regulations;

I. Intentionally Omitted; and

J. Be registered as a business entity licensed to do business in the State, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies when onsite at Customer's facilities including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at **https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf**. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents, and subcontractors. It is mutually agreed by the Parties that ISO27001 and SOC II Type 2 satisfy the requirements stated in this Section 9.2.

9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with, if required by applicable law, applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.

9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum standards as found in the Contract.

9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

9.8 Intentionally Omitted.

9.9 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.10 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents may be configured by Customer to comply with the applicable requirements of Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents subject to Section 508 lack such functionality, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

Notwithstanding the foregoing, Customer is solely responsible to configure the services to comply with the applicable requirements.

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Upon thirty (30) days advance notice, Supplier will permit Customer, or its representative under confidentiality obligations, to remotely review Supplier's records and information regarding fees under the Agreement. Any such audit will be conducted during normal business hours and in a manner designed to cause minimal impact on Supplier's ordinary business activities.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3 Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director. The Order Form will explicitly state when such items are subject to this Section 10.3.

11 Confidentiality

11.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or

any other persons or entities without Customer's prior express written permission or as otherwise permitted under the Contract Documents. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall promptly report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and, subject to Section 16.5 below, shall bear all legally required costs associated with the investigation, response and recovery in connection with any Supplier's breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent

company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall promptly forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall reasonably cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request. Notwithstanding the foregoing, Supplier may disclose data or records to its employees or subcontractors who are subject to confidentiality obligations substantially similar to those found herein and only on a need to know basis.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Except as set forth herein, the Customer will protect all Supplier Confidential Information as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that (i) the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy and (ii) the

Customer discloses only such information as is required by law. Customer acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any Supplier Confidential Information to others may cause immediate and irreparable harm to Supplier and certain beneficiaries and may violate state or federal laws and regulations. If the Customer or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, Supplier will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State under law or Contract. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall be subject to Section 16.5 below.

13 Assignment and Permitted Subcontractors

13.1 Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said

corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 Supplier is permitted to utilize subcontractors and subprocessors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees, subprocessors and subcontractors and for payments to such persons or entities. Qualtrics' list of subprocessors in place on the effective date of the Agreement is published by Qualtrics at www.qualtrics.com/subprocessor-list or Qualtrics will make it available to Customer upon request, including the name, address and role of each Subprocessor Qualtrics uses to provide the Cloud Service. For any other subcontractor utilized by Supplier in its performance of this Agreement, prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. As part of the approval request, and upon Customer's request, Supplier will provide the entity name, and employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred in whole, at no additional cost unless professional services are required, to other Customer entities.

14 Background Checks and Criminal History Investigations

Utilizing the services of Sterling Talent Solutions, Qualtrics performs the following background checks (to the extent permitted by local law) on applicants prior to employment:

- Criminal Felony & Misdemeanor
- Education Report
- Employment Report
- I-9 Employment Eligibility
- SSN Trace
- SSN Validation
- National Criminal Search (7 years)
- Global Sanctions

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the

right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any grossly negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier

and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier, nor will Supplier be liable to the State or any Customer for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, the maximum aggregate liability of either party to the other will not exceed three times the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period for any damages, expenses, costs, actions, claims, and liabilities arising from or related to (a) property damage, bodily injury or death caused by either party; (b) indemnity, security or confidentiality obligations under the Contract; or (c) the bad faith, gross negligence, intentional

misconduct or other acts for which applicable law does not allow exemption from liability of either party.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

D. Subject to 16.5 (A) and (B), the maximum aggregate liability of either party to the other or any other person or entity for all events (or series of connected events) arising in any twelve-month period will not exceed three times (3x) the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve-month period. Any "twelve-month period" commences on the Subscription Term start date or any of its yearly anniversaries.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with

such termination. Any amount paid to Supplier in the form of prepaid fees and shall be responsible for payment of amounts incurred up to the date of such termination. that are unused when the Contractor certain obligations are terminated shall be refunded.

17.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

18.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract or ; (ii) Supplier's material breach subject to a condition precluding cure within the thirty (30) day notice period.

18.3 Upon receipt of notice of a termination pursuant to this Section 18 from Customer or the State, Supplier shall take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. Termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts to the State or Customer when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

19.1 The State may not terminate the Contract, in whole or in part, for convenience.

19.2 Intentionally Omitted.

20 Suspension of Supplier

20.1 Intentionally Omitted.

20.2 Intentionally Omitted.

20.3 Intentionally Omitted.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance (other than for the payments of amounts due) if delayed as a result of causes beyond its reasonable control provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's commercially reasonable control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a Contract may be terminated in the event conditions beyond the performing party's reasonable control render the Cloud Service unavailable for more than fifteen (15) consecutive days (in which case Customer will receive a refund of prepaid fees starting from the beginning of the period of unavailability due to such conditions).

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event or caused by Customer's breach of the Contract and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and

security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below (or such individuals as configured by Customers in the Cloud Services as the Brand Admin). Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:
State Purchasing Director
5005 North Lincoln Boulevard, Suite 300
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
5005 North Lincoln Boulevard, Suite 300
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State of Oklahoma without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Intentionally Omitted

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Neither party will use the name of the other party in publicity activities without the prior written consent of the other.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq*. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required; provided that Customer (i) gives Supplier reasonable written notice to allow Supplier to seek a protective order or other appropriate remedy (except to the extent Customer's compliance with the foregoing would cause it to violate a legal requirement), and (ii) discloses only such information as is required by law.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D. Intentionally Omitted.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration, but shall continue to be governed by the terms of the Contract until expiration of such agreements. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier’s representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Supplier and Customer shall comply with Export Laws in the performance of this Agreement. Supplier Confidential Information is subject to Export Laws. Customer, its Affiliates, and Authorized Users shall not directly or indirectly export, re-export, release, or transfer Confidential Information in violation of Export Laws. Customer is solely responsible for compliance with Export Laws related to Customer Data, including obtaining any required export

authorizations for Customer Data. Customer shall not use the Cloud Service from Crimea/Sevastopol, Cuba, Iran, the People's Republic of Korea (North Korea) or Syria.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT #1056 TERMS

1. Statewide Contract Type

1.1 The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.

1.2 The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

2.1 Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written Order Forms by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

2.2 Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

2.3 Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

3.1. Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

3.2. 17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees and shall be responsible for payment of amounts incurred up to the date of such termination. that are unused when the Contractor certain obligations are terminated shall be refunded.

3.3. The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

4. Termination for Cause

4.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights

and obligations of any party regarding portions of the Contract that are not terminated.

4.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract or ; (ii) Supplier's material breach subject to a condition precluding cure within the thirty (30) day notice period.

4.3 Upon receipt of notice of a termination pursuant to this Section 4 from Customer or the State, Supplier shall take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. Termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

4.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts to the State or Customer when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

5. Termination for Convenience

5.1 The State may not terminate the Contract, in whole or in part, for convenience.

5.2 Intentionally Omitted.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to **strategic.sourcing@omes.ok.gov**;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;

b. April 01 through June 30;

c. July 01 through September 30; and

d. October 01 through December 31.

v. Reports must include the following information:

a. Procuring entity;
b. Order date;
c. Purchase Order number or note that the transaction was paid by Purchase Card;
d. City in which products or services were received or specific office or subdivision title;
e. Product manufacturer or type of service;
f. Manufacturer item number, if applicable;
g. Product description;
h. General product category, if applicable;
i. Quantity;
j. Unit list price or MSRP, as applicable;
k. Unit price charged to the purchasing entity; and
l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services ("OMES-IS") is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

1.1 **COTS** means software that is commercial off the shelf.

1.2 **Customer Data** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include Supplier's Confidential Information.

1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.

1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.

1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.8 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.9 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.

1.10 **State CIO** means the State Chief Information Officer or authorized designee.

1.11 **Supplier Intellectual Property** means i) the Cloud Service, Documentation, and Cloud Materials, and (ii) information regarding Qualtrics research and development, product offerings, pricing and availability.

1.12 **Third-Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

1.13 **Intentionally Omitted.**

2 Support

Qualtrics shall respond to technical support requests 24 hours a day, 7 days a week, excluding major international holidays. Qualtrics shall respond to submitted support cases (also referred to as "case", "incident", or "issue") as described in the table below.

Priority	Definition	Response Level
P1	**Very High**: An incident should be categorized with the priority "very high" if the problem has very serious consequences for normal business processes or IT processes related to core business processes. Urgent work cannot be performed. This is generally caused by the following circumstances:	**Initial Response:** Within one hour of case submission (must elect response by phone).

	- A productive service is completely down. - The imminent system Go-Live or upgrade of a production system cannot be completed. - The customer's core business processes are seriously affected. A workaround is not available for each circumstance. The incident requires immediate processing because the malfunction may cause serious losses.	
P2	**High**: An incident should be categorized with the priority "high" if normal business processes are seriously affected. Necessary tasks cannot be performed. This is caused by incorrect or inoperable functions in the Qualtrics service that are required immediately. The incident is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.	**Initial Response:** Within four hours of case submission (must submit via phone).
P3	**Medium**: An incident should be categorized with the priority "medium" if normal business processes are affected. The problem is caused by incorrect or inoperable functions in the Qualtrics service.	**Initial Response:** Within one business day of case submission.
P4	**Low**: An incident should be categorized with the priority "low" if the problem has little or no effect on normal business processes. The problem is caused by incorrect or inoperable functions in the Qualtrics service that are not required daily, or are rarely used.	**Initial Response:** Within two business days of case submission.

The following types of incidents are excluded from customer response levels as described above: (i) incidents regarding a release, version and/or functionalities of Cloud Services developed specifically for customer (including those custom developed or individual content services); (ii) the root cause behind the incident is not a malfunction, but missing functionality ("development request") or (iii) the incident is ascribed to a consulting request ("how-to").

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

2.1 Customer removes the product for which the services are provided, from productive use or;

2.2 The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

Any termination under this Section 2 shall be without refund and on the condition that all fees set forth in the applicable Order Form are paid in full.

3 Compliance and Electronic and Information Technology Accessibility

Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

Customer Data may only be processed outside of the data center region for:

1. Certain technical support e.g. if a user calls outside of their main data center region's timezone, or where technical support agents expertise are required from other regions;
2. Where Authorized Users are accessing the Cloud Services or respondents are completing surveys from a location outside of the data center region;
3. Ensuring that the Cloud Service can be made available globally to Customer, its Authorized Users, respondents, website visitors, and mobile application visitors and to improve latency;
4. Where incident response or resolution is required from Qualtrics engineering offices in different data center regions; or
5. The use of sub processors results in processing outside the data center region. Qualtrics list of available subprocessors can be found at www.qualtrics.com/subprocessor-list.

6 Compliance with Technology Policies

6.1 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies when onsite at Customer's facilities including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors. It is mutually agreed by the Parties that ISO27001 and SOC II Type 2 satisfy the requirements stated in this Section 9.2. of Attachment B.

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State. Any such extension is only valid if agreed to by Supplier in a mutually executed Order Form.

9 Intentionally Omitted

10 Commercial Off the Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of a Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

The State retains all rights in and related to Customer Data. Supplier may use Customer-provided trademarks solely to provide and support the Cloud Service.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

12.1 Supplier, Supplier's Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to the State are reserved to Supplier and its licensors.

12.2 Customer retains all rights in and related to the Customer Data. Qualtrics may use Customer-provided trademarks solely to provide and support the Cloud Service.

13 Hosting Services

13.1 If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise, if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

A minimum of five days' advance notice will be provided by email to Customer for all required system maintenance as determined by Qualtrics ("Scheduled Maintenance") exceeding two hours. For Scheduled Maintenance lasting less than two hours, notice will be displayed on the login page. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals (or such individuals as configured by Customers in the Cloud Services as the Brand Admin) shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer Data without first notifying the Customer within a reasonable time to allow Customer to seek a protective order or other appropriate remedy (except to the extent Supplier's compliance with the foregoing would cause it to violate a court order or other legal requirement). In addition, Supplier shall only disclose such information as is required by the governmental entity or otherwise required by law and shall use commercially reasonable efforts to obtain confidential treatment for any Customer Data so disclosed. Supplier will reasonably cooperate with Customer in dealing with requests from regulatory authorities regarding Supplier's processing of Personal Data or any Data Breach.

3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier as a result of its negligence or willful misconduct. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to

safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.

3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus, except if such virus is caused by any file uploads by any Authorized Users or respondents.

4. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, not provided by Supplier. Such devices provided by Supplier shall be subject to the terms of the Qualtrics Privacy and Security Framework. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

5. Supplier shall perform due diligence on its data center providers in line with its third party management program. This shall include obtaining and reviewing a Service Organization Control (SOC) 2 audit report or approved equivalent performed by an independent party. Such reports will be shared with the Customer upon request, where the Vendor has permission to do so. Supplier submitted to the review and met the State's minimum-security standards at time the Contract was executed. Failure to maintain the State's minimum-security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes in such a way that is materially worsens the data protection or increases the security risk as compared to the prior year's security risk assessment, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes

a material breach by Supplier and may result in a whole or partial termination of the Contract.

6. Supplier's obligations under the Contract may not be assigned to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

7. Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

8. Supplier is permitted to utilize subcontractors in support of the Contract, and the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. As of the Effective Date of the applicable Contract Document, Supplier's list of subcontractors may be found at https://www.qualtrics.com/subprocessor-list/. Except as set forth herein, prior to a subcontractor being utilized by the Supplier, the Supplier shall notify the State of such subcontractor proposed for use by the Supplier. If Customer has a legitimate reason under applicable law to object to a new subcontractor, Customer may terminate the applicable Order Form (limited to the Cloud Service for which the new subcontractor is intended to be used) on written notice to Supplier. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of Supplier's notice to Customer informing Customer of the new subcontractor. If Customer does not terminate within this 30 day period, Customer is deemed to have accepted the new subcontractor. Any termination under this Section C.4 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

C. Security Incident or Data Breach Notification: Supplier shall inform Customer of any confirmed Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If

a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication, where feasible.

2. Supplier shall report a confirmed Security Incident that involves Customer Data to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation.

3. Supplier shall:

a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;

b. Make summary information regarding such procedures available to Customer at Customer's request;

c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. Upon determination that an actual breach occurs the Supplier has 48 hours to notify the state, or sooner if required by applicable statute.

D. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

2. Unless otherwise stipulated and subject to Section 16.5 of Attachment B, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with, to the extent legally required, (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and

hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

E. Notices

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to (or such individuals as configured by Customers in the Cloud Services as the Brand Admin):

Chief Information Security Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

F. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. Supplier has all rights to provide the Cloud Services.

2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program, provided that Supplier shall not be responsible for any such malicious code placed on the Hosted Services by Customer or its Authorized users.

G. Indemnity

H. Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's gross negligence or willful misconduct. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software, (ii) replace or modify the software with a like or similar product so that it becomes non-infringing, or (iii) if options (i) and (ii) are not reasonably available, Supplier or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other. Supplier's obligations under this Section H will not apply if the claim results from (i) Customer's breach of Supplier's Usage Rights and Restrictions, (ii) use of the Cloud Service in conjunction with any product or service not provided by Supplier, or (iii) use of the Cloud Service provided for no fee.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall provide for an orderly return of Customer Data in a common format specified by the Customer and, as determined by the Customer:

a. return upon request the Customer Data to Customer at no additional cost, with no undue delay and the subsequent secure disposal of State Data;

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist	Compliance checklist –
Policy Area 1	Information Exchange Agreements
Policy Area 2	Security Awareness Training
Policy Area 3	Incident Response
Policy Area 4	Auditing and Accountability
Policy Area 5	Access Control
Policy Area 6	Identification and Authentication
Policy Area 7	Configuration Management
Policy Area 8	Media Protection
Policy Area 9	Physical Protection
Policy Area 10	Systems and Communications Protection and Information Integrity
Policy Area 11	Formal Audits
Policy Area 12	Personnel Security

Attachment E, Ex-1 Qualtrics General T&Cs for Cloud Services ("GTC")

GENERAL TERMS AND CONDITIONS FOR QUALTRICS CLOUD SERVICES ("GTC")

Between	**Qualtrics, LLC** **(an SAP America Inc. company)** **333 W. River Park Drive** **Provo, Utah 84604** **("Qualtrics")**
And	**[Customer Name]** **[Customer Address]** **("Customer")**

1. DEFINITIONS

Capitalized terms used in this document are defined in the Glossary.

2. USAGE RIGHTS AND RESTRICTIONS

2.1 Grant of Rights.

Qualtrics grants to Customer a non-exclusive, non-transferable and world-wide right to use the Cloud Service (including its implementation and configuration), Cloud Materials (as applicable) and Documentation solely for Customer's and its Affiliates' internal business operations. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.

2.2 Authorized Users.

Customer may permit Authorized Users to use the Cloud Service. Usage is limited to the Usage Metrics and volumes stated in the Order Form. Access credentials for the Cloud Service may not be used by more than one individual, but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

2.3 Acceptable Use Policy.

With respect to the Cloud Service, Customer will not:

(a) disassemble, decompile, reverse-engineer, copy, translate or make derivative works,

(b) transmit any content or data that is unlawful or infringes any intellectual property rights, or

(c) circumvent or endanger its operation or security.

2.4 Verification of Use.

Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume. Qualtrics may monitor use to verify compliance with Usage Metrics, volume and the Agreement.

2.5 Suspension of Cloud Service.

Qualtrics may suspend or limit use of the Cloud Service if continued use may result in material harm to the Cloud Service or its users. Qualtrics will promptly notify Customer of the suspension or limitation. Qualtrics will limit a suspension or limitation in time and scope as reasonably possible under the circumstances.

2.6 Third Party Web Services.

The Cloud Service may include integrations with web services made available by third parties (other than Qualtrics' Affiliates) that are accessed through the Cloud Service and subject to terms and conditions with those third parties. These third party web services are not part of the Cloud Service and the Agreement does not apply to them.

2.7 Mobile Access to Cloud Service.

If applicable, Authorized Users may access certain Cloud Services through mobile applications obtained from third-party websites such as Android or Apple app store. The use of mobile applications may be governed by the terms and conditions presented upon download/access to the mobile application and not by the terms of the Agreement.

3. QUALTRICS RESPONSIBILITIES

3.1 Provisioning.

Qualtrics provides access to the Cloud Service as described in the Agreement.

3.2 Support.

Qualtrics provides support for the Cloud Service as referenced in the Order Form.

3.3 Security.

Qualtrics will implement and maintain appropriate technical and organizational measures to protect the personal data processed by Qualtrics as part of the Cloud Service as described in the Data Processing Agreement attached hereto as **Exhibit A** ("**DPA**") for Cloud Services incorporated into the Order Form in compliance with applicable data protection law.

3.4 Modifications.

(a) The Cloud Service and Qualtrics Policies may be modified by Qualtrics. Qualtrics will inform Customer of modifications by email, the support portal, release notes, Documentation or the Cloud Service. The information will be delivered by email if the modification is not solely an enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.

(b) If Customer establishes that a modification is not solely an enhancement and materially reduces the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to Qualtrics within thirty days after receipt of Qualtrics' informational notice.

3.5 Analyses.

Qualtrics or Qualtrics' Affiliates may create analyses utilizing, in part, Customer Data and information derived from Customer's use of the Cloud Service and Consulting Services, as set forth below ("**Analyses**"). Analyses will anonymize and aggregate information and will be treated as Cloud Materials.

Unless otherwise agreed, personal data contained in Customer Data is only used to provide the Cloud Service and Consulting Services. Analyses may be used for the following purposes:

a) product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new Qualtrics products and services,
b) improving resource allocation and support,
c) internal demand planning,
d) training and developing machine learning algorithms,
e) improving product performance,
f) verification of security and data integrity
g) identification of industry trends and developments, creation of indices and anonymous benchmarking

4. CUSTOMER AND PERSONAL DATA

4.1 Customer Data.

Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to Qualtrics (including Qualtrics' Affiliates and subcontractors) a nonexclusive right to process Customer Data solely to provide and support the Cloud Service.

4.2 Personal Data.

Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data privacy and protection laws and as agreed to under the Contract.

4.3 Security.

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct or authorize penetration tests of the Cloud Service without advance approval from Qualtrics.

4.4 Access to Customer Data.

(a) During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Qualtrics and Customer will find a reasonable method to allow Customer access to Customer Data.

(b) Before the Subscription Term expires, if available, Customer may use Qualtrics' self-service export tools (as available) to perform a final export of Customer Data from the Cloud Service. Alternatively, Customer may request data export through support ticket.

(c) At the end of the Agreement, Qualtrics will delete the Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.

(d) In the event of third party legal proceedings relating to the Customer Data, Qualtrics will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

5. FEES AND TAXES

5.1 Fees and Payment.

Customer will pay fees as stated in the Order Form. After prior written notice, Qualtrics may suspend Customer's use of the Cloud Service until payment is made. Customer cannot withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable and fees non-refundable.

5.2 Taxes.

Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than Qualtrics' income and payroll taxes. Customer must provide to Qualtrics any direct pay permits or valid tax-exempt certificates prior to signing an Order Form. If Qualtrics is required to pay taxes (other than its income and payroll taxes), Customer will reimburse Qualtrics for those amounts and indemnify Qualtrics for any taxes and related costs paid or payable by Qualtrics attributable to those taxes.

6. TERM AND TERMINATION

6.1 Term.

The Subscription Term is as stated in the Order Form.

6.2 Termination.

(a) In addition to any other termination rights in the Contract, A party may terminate the Agreement as permitted under Sections 3.4(b), 7.3(b), 7.4(c), or 8.1(c) (with termination effective thirty days after receipt of notice in each of these cases).

6.3 Refund and Payments. Reserved.

6.4 Effect of Expiration or Termination.

Upon the effective date of expiration or termination of the Agreement:

(a) Customer's right to use the Cloud Service and all Qualtrics Confidential Information will end,

(b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and

(c) termination or expiration of the Agreement does not affect other agreements between the parties.

6.5 Survival.

Sections 1, 5, 6.3, 6.4, 6.5, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

7. WARRANTIES

7.1 Compliance with Law.

Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:

(a) in the case of Qualtrics, the operation of Qualtrics' business as it relates to the Cloud Service, and

(b) in the case of Customer, the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices.

Qualtrics warrants that it will provide the Cloud Service:

(a) in substantial conformance with the Documentation; and

(b) with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service.

7.3 Remedy.

Unless otherwise required by applicable law or otherwise provided under the Contract, Customer's sole and exclusive remedies and Qualtrics' entire liability for breach of the warranty under Section 7.2 will be:

(a) the re-performance of the deficient Cloud Service, and

(b) if Qualtrics fails to re-perform, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three months of Qualtrics' failure to re-perform.

7.4 System Availability.

(a) Qualtrics warrants to maintain an average monthly system availability for the production system of the Cloud Service as defined in the applicable service level agreement or Supplement ("SLA").

(b) Customer's sole and exclusive remedy for Qualtrics' breach of the SLA is the issuance of a credit in the amount described in the SLA. Customer will follow Qualtrics' posted credit claim procedure. When the validity of the service credit is confirmed by Qualtrics in writing (email permitted), Customer may apply the credit to a future invoice for the Cloud Service or request a refund for the amount of the credit if no future invoice is due.

(c) In the event Qualtrics fails to meet the SLA (i) for four consecutive months, or (ii) for five or more months during any twelve months period, or (iii) at a system availability level of at least 95% for one calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing Qualtrics with written notice within thirty days after the failure.

7.5 Warranty Exclusions.

The warranties in Sections 7.2 and 7.4 will not apply if:

(a) the Cloud Service is not used in accordance with the Agreement or Documentation,

(b) any non-conformity is caused by Customer, or by any product or service not provided by Qualtrics, or

(c) the Cloud Service was provided for no fee.

7.6 Disclaimer.

Except as expressly provided in the Agreement, neither Qualtrics nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of Qualtrics or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1 Claims Brought Against Customer.

(a) Qualtrics will defend Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's and its Affiliates' use of the Cloud Service infringes or misappropriates a patent claim, copyright, or trade secret right. Qualtrics will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement Qualtrics enters into) with respect to these claims.

(b) Qualtrics' obligations under Section 8.1 will not apply if the claim results from (i) Customer's breach of Section 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by Qualtrics, or (iii) use of the Cloud Service provided for no fee.

(c) In the event a claim is made or likely to be made, Qualtrics may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, Qualtrics or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

8.2 Claims Brought Against Qualtrics. Reserved.

8.3 Third Party Claim Procedure.

(a) The party against whom a third party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.

(b) The party that is obligated to defend a claim will have the right to fully control the defense.

(c) Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought.

8.4 Exclusive Remedy.

9. LIMITATION OF LIABILITY. Reserved.

9.1 Unlimited Liability.
9.2 Liability Cap.
9.3 Exclusion of Damages.
9.4 Risk Allocation.

The Agreement allocates the risks between Qualtrics and Customer. The fees for the Cloud Service and Consulting Services reflect this allocation of risk and limitations of liability.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 QUALTRICS Ownership.

Qualtrics, Qualtrics' Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to Qualtrics and its licensors.

10.2 Customer Ownership.

Customer retains all rights in and related to the Customer Data. Qualtrics may use Customer-provided trademarks solely to provide and support the Cloud Service.

10.3 Non-Assertion of Rights.

Customer covenants, on behalf of itself and its successors and assigns, not to assert against Qualtrics and its Affiliates or licensors, any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Consulting Services.

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

(a) The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.

(b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.

(c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.

11.2 Exceptions.

The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:

(a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,

(b) is generally available to the public without breach of the Agreement by the receiving party,

(c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or

(d) the disclosing party agrees in writing is free of confidentiality restrictions.

11.3 Publicity.

Neither party will use the name of the other party in publicity activities without the prior written consent of the other.

12. MISCELLANEOUS

12.1 Severability.

If any provision of the Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

12.2 No Waiver.

A waiver of any breach of the Agreement is not deemed a waiver of any other breach.

12.3 Electronic Signature.

Electronic signatures that comply with applicable law are deemed original signatures.

12.4 Regulatory Matters.

Qualtrics Confidential Information is subject to export control laws of various countries, including the laws of the United States and Germany. Customer will not submit Qualtrics Confidential Information to any government agency for licensing consideration or other regulatory approval, and will not export Qualtrics Confidential Information to countries, persons or entities if prohibited by export laws.

12.5 Notices.

All notices will be in writing and given when delivered to the address set forth in an Order Form with copy to the legal department. Notices by Qualtrics relating to the operation or support of the Cloud Service and those under Sections 3.4 and 5.1 may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Order Form.

12.6 Assignment.

Without Qualtrics' prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. Qualtrics may assign the Agreement to Qualtrics Affiliates.

12.7 Subcontracting.

Qualtrics may subcontract parts of the Cloud Service or Consulting Services to third parties. Qualtrics is responsible for breaches of the Agreement caused by its subcontractors.

12.8 Relationship of the Parties.

The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by the Agreement.

12.9 Force Majeure. Reserved.

12.10 Governing Law.

The Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the State of Oklahoma, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in Oklahoma County, Oklahoma. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act (where enacted) will not apply to the Agreement. Either party must initiate a cause of action for any claim(s) relating to the Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

12.11 Entire Agreement.

The Agreement constitutes the complete and exclusive statement of the agreement between Qualtrics and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the Agreement and the parties disclaim any reliance on them. The Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if Qualtrics accepts or does not otherwise reject the purchase order.

Glossary

1.1 **"Affiliate"** of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.

1.2 **"Agreement"** means an Order Form and documents incorporated into an Order Form.

1.3 **"Authorized User"** means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor or representative of

(a) Customer,

(b) Customer's Affiliates, and/or

(c) Customer's and Customer's Affiliates' Business Partners.

1.4 **"Business Partner"** means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.

1.5 **"Cloud Service"** means any distinct, subscription-based, hosted, supported and operated on- demand solution provided by Qualtrics under an Order Form.

1.6 **"Cloud Materials"** mean any materials provided or developed by Qualtrics (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.

1.7 "**Confidential Information**" means

(a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and

(b) with respect to Qualtrics: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding Qualtrics research and development, product offerings, pricing and availability.

(c) Confidential Information of either Qualtrics or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.

1.8 **"Consulting Services"** means professional services, such as implementation, configuration, custom development and training, performed by Qualtrics' employees or subcontractors as described in any Order Form and which are governed by the Supplement for Consulting Services or similar agreement.

1.9 **"Customer Data" Reserved.**

1.10 **"Documentation"** means Qualtrics' then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.

1.11 **"Order Form"** means the ordering document for a Cloud Service that references the GTC.

1.12 **"Qualtrics Policies"** means the operational guidelines and policies applied by Qualtrics to provide and support the Cloud Service as incorporated in an Order Form.

1.13 **"Subscription Term"** means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.

1.14 **"Supplement"** means as applicable, the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.

1.15 **"Usage Metric"** means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.

THE PARTIES ENTER INTO THIS AGREEMENT AS OF THE LAST SIGNATURE DATE BELOW ("GTC EFFECTIVE DATE").

CUSTOMER:	**QUALTRICS, LLC**
By:	**By:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**

Exhibit A
Data Processing Agreement

PERSONAL DATA PROCESSING AGREEMENT FOR QUALTRICS CLOUD SERVICES

This Data Processing Addendum ("DPA") is entered into

BETWEEN

(1) Customer; and

(2) Qualtrics.

1. DEFINITIONS

1.1. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to Qualtrics be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

1.2. **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.3. **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

1.4. **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

1.5. **"GDPR"** means the General Data Protection Regulation 2016/679.

1.6. **"New SCC Relevant Transfer"** means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the New Standard Contractual Clauses.

1.7. **"New Standard Contractual Clauses"** means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.

1.8. **"Personal Data" Reserved**.

1.9. **"Personal Data Breach"** means a confirmed:

a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or

b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.10. **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

1.11. **"SAP"** means SAP SE, Qualtrics parent company.

1.12. **"Schedule"** means the numbered Appendix with respect to the Standard Contractual Clauses (2010) and the numbered Annex with respect to the New Standard Contractual Clauses.

1.13. **"Standard Contractual Clauses (2010)"** means the Standard Contractual Clauses (processors) published by the European Commission, reference 2010/87/EU.

1.14. **"Subprocessor"** or **"sub-processor"** means Qualtrics Affiliates, SAP, SAP Affiliates and third parties engaged by Qualtrics, Qualtrics' Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

1.15. **"Technical and Organizational Measures"** means the technical and organizational measures for the relevant Cloud Service set out in Schedule 2.

1.16. **"Third Country"** means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Purpose and Application

2.1.1. This document ("DPA") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Qualtrics and Customer.

2.1.2. This DPA applies to Personal Data processed by Qualtrics and its Subprocessors in connection with its provision of the Cloud Service.

2.1.3. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by Qualtrics. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects (Schedule 1) and the applicable Technical and Organizational Measures (Schedule 2).

2.3. Governance

2.3.1. Qualtrics acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA.

2.3.2. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Qualtrics as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where Qualtrics informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Applicability of the Technical and Organizational Measures

Qualtrics has implemented and will apply the Technical and Organizational Measures. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

3.2. Changes

3.2.1. Qualtrics applies the Technical and Organizational Measures to Qualtrics' entire customer base hosted out of the same data center or receiving the same Cloud Service. Qualtrics may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3.2.2. Qualtrics will publish updated versions of the Technical and Organizational Measures at www.qualtrics.com/terms-of-service.

4. QUALTRICS OBLIGATIONS

4.1. Instructions from Customer

Qualtrics will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. Qualtrics will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or Qualtrics otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Qualtrics will immediately notify Customer (email permitted).

4.2. Processing on Legal Requirement

Qualtrics may also process Personal Data where required to do so by applicable law. In such a case, Qualtrics shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, Qualtrics and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Qualtrics and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Cooperation

4.4.1. At Customer's request, Qualtrics will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Qualtrics' processing of Personal Data or any Personal Data Breach.

4.4.2. If Qualtrics receives a request from a Data Subject in relation to the Personal Data processing hereunder, Qualtrics will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

4.4.3. In the event of a dispute with a Data Subject as it relates to Qualtrics' processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably co-operate with the aim of resolving the dispute amicably with the Data Subject.

4.4.4. Qualtrics shall provide functionality for production systems that supports Customer's ability to correct, delete or anonymize Personal Data from a Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Qualtrics will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. Personal Data Breach Notification

Qualtrics will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Qualtrics may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Qualtrics.

4.6. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, Qualtrics will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports and certifications). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Qualtrics and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, Customer may use Qualtrics' self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs Qualtrics to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer or its independent third party auditor reasonably acceptable to Qualtrics (which shall not include any third party auditors who are either a competitor of Qualtrics or not suitably qualified or independent) may audit Qualtrics' control environment and security practices relevant to Personal Data processed by Qualtrics only if:

a) Qualtrics has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through

providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or Qualtrics;

b) a Personal Data Breach has occurred;
c) an audit is formally requested by Customer's data protection authority; or
d) provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by Qualtrics on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Qualtrics.

6.4. Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by Qualtrics of this DPA, then Qualtrics shall bear its own expenses of an audit. If an audit determines that Qualtrics has breached its obligations under the DPA, Qualtrics will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

Qualtrics is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a) Qualtrics or Qualtrics affiliates on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Qualtrics shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;
b) Qualtrics will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and
c) Qualtrics' list of Subprocessors in place on the effective date of the Agreement is published by Qualtrics at www.qualtrics.com/subprocessor-list or Qualtrics will make it available to Customer upon request, including the name, address and role of each Subprocessor Qualtrics uses to provide the Cloud Service.

7.2. New Subprocessors

Qualtrics' use of Subprocessors is at its discretion, provided that:

a) Qualtrics will inform Customer in advance (by email or by posting on the Cloud Service) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and
b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to Qualtrics. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor. If Customer

does not terminate within this 30 day period, Customer is deemed to have accepted the new Subprocessor.

7.3.2. Within the 30 day period from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for termination and do not affect Qualtrics' right to use the new Subprocessor(s) after the 30 day period.

7.3.3. Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4. Emergency Replacement

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

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

Qualtrics shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2. Applicability of the Standard Contractual Clauses (2010)

8.2.1. Where, for the period up to and including 26 September 2021, Personal Data of a Controller that is subject to GDPR is processed in a Third Country, or where Personal Data of a Swiss or United Kingdom based Controller or another Controller is processed in a Third Country and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses (2010), then:

Qualtrics and Customer enter into the Standard Contractual Clauses (2010);

Customer joins the Standard Contractual Clauses (2010) entered into by Qualtrics or Qualtrics SE and the Subprocessor as an independent owner of rights and obligations; or

Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses (2010) with Qualtrics or the relevant Subprocessors in the same manner as Customer in accordance with Section 8.2.1 a) and b) above. In such case, Customer will enter into the Standard Contractual Clauses (2010) on behalf of the other Controllers.

8.2.2. The Standard Contractual Clauses (2010) shall be governed by the law of the country in which the relevant Controller is established.

8.2.3. Where applicable Data Protection Law adopts the New Standard Contractual Clauses as meeting any required adequacy means as an alternative or update to the Standard Contractual Clauses (2010) then the New Standard Contractual Clauses shall apply in accordance with Section 8.3.

8.3. Applicability of New Standard Contractual Clauses

8.3.1. The following shall apply with effect from 27 September 2021 and shall solely apply in respect of New SCC Relevant Transfers:

8.3.1.1. Where Qualtrics is not located in a Third Country and acts as a data exporter, Qualtrics has entered in to the New Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the New Standard Contractual Clauses shall apply to such New SCC Relevant Transfers.

8.3.1.2. Where Qualtrics is located in a Third Country:

Qualtrics and Customer hereby enter into the New Standard Contractual Clauses with Customer as the data exporter and Qualtrics as the data importer which shall apply as follows:

a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and
b) Module 3 (Processor to Processor) shall apply where Customer is a Processor. Where Customer acts as Processor under Module 3 (Processor to Processor) of the New Standard Contractual Clauses, Qualtrics acknowledges that Customer acts as Processor under the instructions of its Controller(s).

8.3.2. Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer

under the Agreement may also enter into the New Standard Contractual Clauses with Qualtrics in the same manner as Customer in accordance with Section 8.3.1.2 above. In such case, Customer enters into the New Standard Contractual Clauses on behalf of the other Controllers or Processors.

8.3.3. With respect to a New SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the New Standard Contractual Clauses entered into between Customer and Qualtrics (including the relevant Schedules), available to Data Subjects.

8.3.4. The governing law of the New Standard Contractual Clauses shall be the law of Germany.

8.4. Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses (2010) or the New Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the Standard Contractual Clauses (2010) and the New Standard Contractual Clauses.

8.5. Third Party Beneficiary Right under the New Standard Contractual Clauses

8.5.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the New Standard Contractual Clauses and Qualtrics is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right:

8.5.2. In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Cloud Service solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs Qualtrics to erase or return the Personal Data.

9. DOCUMENTATION; RECORDS OF PROCESSING

9.1. Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

1. A. LIST OF PARTIES

1.1. Under the Standard Contractual Clauses (2010)

1.1.1. Data Exporter
The data exporter under the Standard Contractual Clauses (2010) is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also data exporters.

1.1.2. Data Importer
Qualtrics and its Subprocessors that provide and support the Cloud Service are data importers under the Standard Contractual Clauses (2010).

1.2. Under the New Standard Contractual Clauses

1.2.1. Module 2: Transfer Controller to Processor
Where Qualtrics is located in a Third Country, Customer is the Controller and Qualtrics is the Processor, then Customer is the data exporter and Qualtrics is the data importer.

1.2.2. Module 3: Transfer Processor to Processor
Where Qualtrics is located in a Third Country, Customer is a Processor and Qualtrics is a Processor, then Customer is the data exporter and Qualtrics is the data importer.

2. B. DESCRIPTION OF TRANSFER

2.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

2.2. Data Categories

The transferred Personal Data concerns the following categories of data:
Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service.

2.3. Special Data Categories (if agreed)

2.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("Sensitive Data"). Qualtrics has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.

2.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

a) training of personnel;
b) encryption of data in transit and at rest;
c) system access logging and general data access logging.

2.3.3. In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

2.4. Purposes of the data transfer and further processing; Nature of the processing

2.4.1. The transferred Personal Data is subject to the following basic processing activities:

a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support);
b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
c) provision of professional services;
d) communication to Authorized Users;
e) storage of Personal Data in dedicated data centers (multi-tenant architecture);
f) release, development and upload of any fixes or upgrades to the Cloud Service;
g) back up and restoration of Personal Data stored in the Cloud Service;
h) computer processing of Personal Data, including data transmission, data retrieval, data access;
i) network access to allow Personal Data transfer;
j) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;
k) security monitoring, network-based intrusion detection support, penetration testing; and
l) execution of instructions of Customer in accordance with the Agreement.

2.4.2. The purpose of the transfer is to provide and support the Cloud Service. Qualtrics and its Subprocessors may support the Cloud Service data centers remotely. Qualtrics and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

2.5. Additional description in respect of the New Standard Contractual Clauses:

2.5.1. Applicable Modules of the New Standard Contractual Clauses

a) Module 2: Transfer Controller to Processor
b) Module 3: Transfer Processor to Processor

2.5.2. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
In respect of the New Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

2.5.3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Transfers shall be made on a continuous basis.

2.5.4. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.
Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

3. C. COMPETENT SUPERVISORY AUTHORITY

3.1. In respect of the New Standard Contractual Clauses:

3.1.1. Module 2: Transfer Controller to Processor
3.1.2. Module 3: Transfer Processor to Processor

3.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the New Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

Qualtrics will apply and maintain the Technical and Organizational Measures.

To the extent that the provisioning of the Cloud Service comprises New SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define Qualtrics' current technical and organizational measures. Qualtrics may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- Qualtrics protects its assets and facilities using the appropriate means based on the Qualtrics Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Qualtrics buildings must register their names at reception and must be accompanied by authorized Qualtrics personnel.
- Qualtrics employees and external personnel must wear their ID cards at all Qualtrics locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- Qualtrics and all third-party Data Center providers log the names and times of authorized personnel entering Qualtrics' private areas within the Data Centers.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the Qualtrics Security Policy
- All personnel access Qualtrics' systems with a unique identifier (user ID).
- Qualtrics has procedures in place so that requested authorization changes are implemented only in accordance with the Qualtrics Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
- Qualtrics has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Qualtrics uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant
- security updates. Full remote access to Qualtrics' corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- As part of the Qualtrics Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Qualtrics uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Qualtrics Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, Qualtrics conducts internal and external security checks and penetration tests on its IT systems.
- An Qualtrics security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Qualtrics to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over Qualtrics internal networks is protected according to Qualtrics Security Policy.
- When data is transferred between Qualtrics and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Qualtrics-controlled systems (e.g. data being transmitted outside the firewall of the Qualtrics Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Qualtrics data processing systems.

Measures:

- Qualtrics only allows authorized personnel to access Personal Data as required in the course of their duty.
- Qualtrics has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Qualtrics or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- Qualtrics uses controls and processes to monitor compliance with contracts between Qualtrics and its customers, subprocessors or other service providers.
- As part of the Qualtrics Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- All Qualtrics employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Qualtrics customers and partners.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Qualtrics employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- Qualtrics uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- Qualtrics has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Measures:

- Qualtrics uses the technical capabilities of the deployed software (for example: multi- tenancy, system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

Qualtrics has implemented a multi-layered defense strategy as a protection against unauthorized modifications. In particular, Qualtrics uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

PUBLIC SECTOR ADDENDUM TO THE GENERAL TERMS AND CONDITIONS FOR QUALTRICS CLOUD SERVICES ("Public Sector Addendum")

Between	**Qualtrics, LLC** **(an SAP America Inc. company)** **333 W. River Park Drive** **Provo, Utah 84604** **("Qualtrics")**
And	**[Customer Name]** **[Customer Address]** **("Customer")**

The Parties entered into the General Terms and Conditions for Qualtrics Cloud Services dated as of even date herewith (the "**GTC**"), and the Parties desire to amend certain terms of the GTC.

The Parties hereby agree as follows:

1. **Definitions**
   All capitalized terms used but not defined herein have the meanings given to them in the GTC.

2. **Section Headings**
   All Sections will retain their headings unless otherwise indicated herein.

3. **Section 5.2 of the GTC is hereby deleted and replaced in its entirety by the following:**
   Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than Qualtrics' income and payroll taxes. Notwithstanding the foregoing, Customer will not be responsible for taxes from which they are exempt on the condition that Customer presents a direct pay permit or valid tax-exempt certificate for such taxes prior to invoice. If Qualtrics is required to pay taxes (other than its income and payroll taxes), Customer will reimburse Qualtrics for those amounts and, to the extent not prohibited by applicable law, indemnify Qualtrics for any taxes and related costs paid or payable by Qualtrics attributable to those taxes.

4. **Reserved.**

5. **Reserved.**

6. **Reserved.**

7. **Reserved.**

8. **Reserved.**

9. **The following Section 11.4 is hereby added to the GTC:**
   11.4 Disclosure on Legal Requirement
   The receiving party may disclose Confidential Information as required by law (including as required by The Freedom of Information Act, 5 U.S.C. § 552 or analogous state law), provided that the receiving party (i) gives the disclosing party reasonable written notice to allow the disclosing party to seek a protective order or other appropriate remedy (except to the extent the receiving party's compliance with the foregoing would cause it to violate a legal requirement), and (ii) discloses only such information as is required by law.

10. **Section 12.6 of the GTC is hereby deleted and replaced in its entirety by the following:**

Neither party shall assign or transfer the Agreement (or any of its rights or obligations) to any party without the prior written consent of the other party, except that either party may assign the Agreement to its Affiliates.

11. **Sections 8.2, 8.3, 8.4, and 8.5 of Exhibit A (Data Processing Agreement) of the GTC and their headings are hereby deleted and replaced by the following new Section 7.2:**

    7.2 Amending the Agreement for International Processing

    The Standard Contractual Clauses and the New Standard Contractual Clauses have been removed from the Agreement. In the event Customer (i) chooses to collect Personal Data of an EEA or Swiss based Controller which is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as a safe country with an adequate level of data protection under Art. 45 GDPR, or (ii) collects Personal Data of another Controller which is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller, Customer shall provide prior notification to Qualtrics and the parties shall amend the Agreement as necessary. Customer's failure to provide notification to Qualtrics in advance of collection of such personal data is a material breach and Qualtrics may choose to terminate the Agreement.

12. **Schedule 1 Description of the Processing of the GTC is hereby deleted and replaced in its entirety with the attached Schedule 1.**

13. **The first three paragraphs of Schedule 2 Technical and Organizational Measures of the GTC are hereby deleted and replaced in their entirety by the following:**

    This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of applicable Data Protection Law.

    Qualtrics will apply and maintain the Technical and Organizational Measures.

THE PARTIES ENTER INTO THIS AGREEMENT AS OF THE LAST SIGNATURE DATE BELOW ("PUBLIC SECTOR ADDENDUM EFFECTIVE DATE").

CUSTOMER:	**QUALTRICS, LLC**
By:	**By:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of applicable Data Protection Law.

1. A. LIST OF PARTIES

1.1. Data Exporter

The data exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also data exporters.

1.2. Data Importer

Qualtrics and its Subprocessors that provide and support the Cloud Service are data importers.

2. B. DESCRIPTION OF TRANSFER

2.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

2.2. Data Categories

The transferred Personal Data concerns the following categories of data:
Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service.

2.3. Special Data Categories (if agreed)

2.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("Sensitive Data"). Qualtrics has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.

2.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

a) training of personnel;
b) encryption of data in transit and at rest;
c) system access logging and general data access logging.

2.3.3. In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

2.4. Purposes of the data transfer and further processing; Nature of the processing

2.4.1. The transferred Personal Data is subject to the following basic processing activities:

a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support);
b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
c) provision of professional services;
d) communication to Authorized Users;
e) storage of Personal Data in dedicated data centers (multi-tenant architecture);
f) release, development and upload of any fixes or upgrades to the Cloud Service;
g) back up and restoration of Personal Data stored in the Cloud Service;

h) computer processing of Personal Data, including data transmission, data retrieval, data access;
i) network access to allow Personal Data transfer;
j) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;
k) security monitoring, network-based intrusion detection support, penetration testing; and
l) execution of instructions of Customer in accordance with the Agreement.

2.4.2. The purpose of the transfer is to provide and support the Cloud Service. Qualtrics and its Subprocessors may support the Cloud Service data centers remotely. Qualtrics and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

2.5. Additional description:

2.5.1. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Transfers shall be made on a continuous basis.

2.5.2. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.
Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

Attach E, Ex-3 Qualtrics LLC Pricing.

The following is valid for the initial 1 year term of this Contract only.

CX SKUs

CX Foundation

Pricing is per user per year

Price Tiers - Users		List Price
Base Spend		**$12,500**
5	24	$2,500
24	49	$1,750
50	74	$1,375
75	99	$1,188
100	124	$1,063
125	149	$975
150	249	$913
250	499	$775
500	999	$625
1000	2499	$500
2500	4999	$388
5000	9999	$313
10000	24999	$250
25000	+	$200

Digital Feedback

Traffic (Page Views)	List
Up to 10M	$0
Up to 25M	$15,000
Up to 50M	$25,000
Up to 75M	$32,813
Up to 100M	$40,000
Up to 200M	$75,000
Up to 300M	$105,000
Up to 400M	$130,000
Up to 500M	$150,000
Up to 750M	$206,250

Up to 1B	$262,500
Up to 2B	$500,000
Up to 3B	$675,000
Up to 4B	$800,000
Up to 5B	$937,500
Up to 7.5B	$1,312,500
Up to 10B	$1,625,000
Up to 12.5B	$1,875,000
Up to 15B	$2,250,000

CustomerXM for Digital

Traffic (Page Views)	List
Up to 10M	$25,000
Up to 25M	$43,750
Up to 50M	$57,500
Up to 75M	$68,125
Up to 100M	$77,500
Up to 200M	$122,500
Up to 300M	$160,000
Up to 400M	$195,000
Up to 500M	$218,750
Up to 750M	$306,250
Up to 1B	$375,000
Up to 2B	$675,000
Up to 3B	$925,000
Up to 4B	$1,075,000
Up to 5B	$1,275,000
Up to 7.5B	$1,712,500
Up to 10B	$2,150,000
Up to 12.5B	$2,525,000
Up to 15B	$2,837,500

Customer Care

Pricing is per user per year

Customer Care		
Price Tiers - Employees		List Price
25	49	$1,925
50	74	$1,549
75	99	$1,363
100	124	$1,238
125	149	$1,138
150	249	$1,075
250	499	$925
500	999	$788
1000	2499	$663
2500	4999	$525
5000	9999	$438
10000	24999	$363
25000	+	$288

Account Management

Pricing is per user per year

Account Management		
Price Tiers - Employees		List Price
25	49	$1,750
50	74	$1,425
75	99	$1,263
100	124	$1,150
125	149	$1,063
150	249	$1,000
250	499	$875
500	999	$738
1000	2499	$613

2500	4999	$488
5000	9999	$411
10000	24999	$338
25000	+	$275

Location

Pricing is per user per year

Locations		
Price Tiers - Employees		List Price
25	49	$1,638
50	74	$1,338
75	99	$1,188
100	124	$1,075
125	149	$1,000
150	249	$936
250	499	$813
500	999	$688
1000	2499	$575
2500	4999	$463
5000	9999	$388
10000	24999	$325
25000	+	$263

Social Connect

Pricing is per user per year

Qualtrics Connect		
Price Tiers - Users		List Price
5	15	$ 8,000
16	50	$ 6,000
51	100	$ 4,500
101	500	$ 3,700

Additional Stream Units (Price at every 10 unit)

Stream Units		List Price
10	40	$ 4,800
50	70	$ 3,600
80+		$ 2,400

EX SKUs

Engagement

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$30.00
Tier 2	2,001 - 5,000	$25.00
Tier 3	5001 - 10,000	$22.00
Tier 4	10,001 - 15,000	$19.00
Tier 5	15,001 - 25,000	$17.00
Tier 6	25,001 - 50,000	$16.00
Tier 7	50,001 - 75,000	$15.00
Tier 8	75,001 - 100,000	$13.50
Tier 9	100,001 +	$12.00

Add On Pulse

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$15.00
Tier 2	2,001 - 5,000	$12.50
Tier 3	5001 - 10,000	$11.00
Tier 4	10,001 - 15,000	$9.50

Tier 5	15,001 - 25,000	$8.50
Tier 6	25,001 - 50,000	$8.00
Tier 7	50,001 - 75,000	$7.50
Tier 8	75,001 - 100,000	$6.56
Tier 9	100,001 +	$5.49

Ad Hoc Employee Research

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$13.50
Tier 2	2,001 - 5,000	$11.25
Tier 3	5,001 - 10,000	$9.90
Tier 4	10,001 - 15,000	$8.55
Tier 5	15,001 - 25,000	$7.65
Tier 6	25,001 - 50,000	$7.20
Tier 7	50,001 - 75,000	$6.75
Tier 8	75,001 - 100,000	$6.08
Tier 9	100,001 +	$5.40

Lifecycle

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$18.00
Tier 2	2,001 - 5,000	$12.00
Tier 3	5001 - 10,000	$10.00
Tier 4	10,001 - 15,000	$8.00
Tier 5	15,001 - 25,000	$7.00
Tier 6	25,001 - 50,000	$6.00
Tier 7	50,001 - 75,000	$5.00
Tier 8	75,001 - 100,000	$4.35
Tier 9	100,001 +	$4.00

Benefits Optimizer

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$12.00
Tier 2	2,001 - 5,000	$6.48
Tier 3	5001 - 10,000	$3.24

Tier 4	10,001 - 15,000	$1.80
Tier 5	15,001 - 25,000	$1.56
Tier 6	25,001 - 50,000	$1.32
Tier 7	50,001 - 75,000	$1.08
Tier 8	75,001 - 100,000	$0.96
Tier 9	100,001 +	$0.84

Employee Technology Experience: Single Project

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$20.00
Tier 2	2,001 - 5,000	$15.30
Tier 3	5001 - 10,000	$12.80
Tier 4	10,001 - 15,000	$10.80
Tier 5	15,001 - 25,000	$9.00
Tier 6	25,001 - 50,000	$6.90
Tier 7	50,001 - 75,000	$6.00
Tier 8	75,001 - 100,000	$5.30
Tier 9	100,001 +	$4.80

Employee Technology Experience: Project Add On

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$10.00
Tier 2	2,001 - 5,000	$7.80
Tier 3	5001 - 10,000	$6.50
Tier 4	10,001 - 15,000	$5.50
Tier 5	15,001 - 25,000	$4.50
Tier 6	25,001 - 50,000	$3.50
Tier 7	50,001 - 75,000	$3.00
Tier 8	75,001 - 100,000	$2.80
Tier 9	100,001 +	$2.50

Employee technology Experience: Enterprise

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$47.00
Tier 2	2,001 - 5,000	$32.40
Tier 3	5001 - 10,000	$27.10
Tier 4	10,001 - 15,000	$25.00

Tier 5	15,001 - 25,000	$21.80
Tier 6	25,001 - 50,000	$18.80
Tier 7	50,001 - 75,000	$16.50
Tier 8	75,001 - 100,000	$14.00
Tier 9	100,001 +	$12.50

360 Development

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$110.40
Tier 2	2,001 - 5,000	$90.00
Tier 3	5001 - 10,000	$69.00
Tier 4	10,001 - 15,000	$57.60
Tier 5	15,001 - 25,000	$51.00
Tier 6	25,001 - 50,000	$45.60
Tier 7	50,001 - 75,000	$36.00
Tier 8	75,001 - 100,000	$31.20
Tier 9	100,001 +	$28.20

Candidate Experience

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$20.00
Tier 2	2,001 - 5,000	$13.20
Tier 3	5,001 - 10,000	$11.00
Tier 4	10,001 - 15,000	$8.80
Tier 5	15,001 - 25,000	$7.70
Tier 6	25,001 - 50,000	$6.60
Tier 7	50,001 - 75,000	$5.50
Tier 8	75,001 - 100,000	$4.79
Tier 9	100,001 +	$4.40

EX Foundation

Pricing is based on per employee per year (USD)

	Employees	List Price
Tier 1	1 - 2,000	$30.00
Tier 2	2,001 - 5,000	$25.00
Tier 3	5,001 - 10,000	$22.00

Tier 4	10,001 - 15,000	$19.00
Tier 5	15,001 - 25,000	$17.00
Tier 6	25,001 - 50,000	$16.00
Tier 7	50,001 - 75,000	$15.00
Tier 8	75,001 - 100,000	$13.50
Tier 9	100,001 +	$12.00

COREXM SKUS

CoreXM Enterprise Advanced

Pricing is per user per year

	Users	List
Tier 1	1-5	$1,440
Tier 2	6-49	$1,320
Tier 3	50-99	$960
Tier 4	100-1,999	$768
Tier 5	2,000-2,999	$600
Tier 6	3,000-3,999	$528
Tier 7	4,000-4,999	$480
Tier 8	5,000+	$444

	Tiers (10K responses)		List
Additional Responses		0.5	$7,000
	1	4	$12,000
	5	10	$9,900
	11	25	$7,000
	26	50	$5,400
	51	+	$4,500

DesignXM Enterprise

Pricing is per user per year

	Users	List
Tier 1	5*	$2,400
Tier 2	6-49	$2,400
Tier 3	50-99	$1,848
Tier 4	100-1,999	$1,500
Tier 5	2,000-2,999	$1,272
Tier 6	3,000-3,999	$1,164
Tier 7	4,000-4,999	$1,056
Tier 8	5,000+	$1,008

DesignXM Digital Feedback

Traffic (Page Views)	List
Up to 10M	$0
Up to 25M	$15,000
Up to 50M	$25,000
Up to 75M	$32,813
Up to 100M	$40,000
Up to 200M	$75,000
Up to 300M	$105,000
Up to 400M	$130,000
Up to 500M	$150,000

Up to 750M	$206,250
Up to 1B	$262,500
Up to 2B	$500,000
Up to 3B	$675,000
Up to 4B	$800,000
Up to 5B	$937,500
Up to 7.5B	$1,312,500
Up to 10B	$1,625,000
Up to 12.5B	$1,875,000
Up to 15B	$2,250,000

DiscoverXM

Pricing is per feedback record per year (USD)

Tier Feedback Records		LIST
minimum	500,000	0.420
500,001	1,000,000	0.310
1,000,001	2,000,000	0.230
2,000,001	4,000,000	0.177
4,000,001	10,000,000	0.127
10,000,001	20,000,000	0.098
20,000,001	40,000,000	0.076
50,000,001	100,000,000	0.065
100,000,001	500,000,000	0.055
500,000,001	1,000,000,000	0.042

EXECUTION VERSION SW1056_Qualtrics

Final Audit Report 2022-10-05

Created:	2022-10-04
By:	Jason Lawson (jason.lawson@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAVvKueqOnw-za0NMqLwhexVgtPpj9Qgmc

"EXECUTION VERSION SW1056_Qualtrics" History

Document created by Jason Lawson (jason.lawson@omes.ok.gov)
2022-10-04 - 7:56:13 PM GMT- IP address: 165.225.216.113

Document emailed to Mark Creer (legal-sales@qualtrics.com) for signature
2022-10-04 - 7:58:35 PM GMT

Email viewed by Mark Creer (legal-sales@qualtrics.com)
2022-10-04 - 7:58:38 PM GMT- IP address: 66.249.92.67

Document e-signed by Mark Creer (legal-sales@qualtrics.com)
Signature Date: 2022-10-05 - 7:56:21 PM GMT - Time Source: server- IP address: 70.103.180.85

Document emailed to Jerry Moore (jerry.moore@omes.ok.gov) for signature
2022-10-05 - 7:56:25 PM GMT

Email viewed by Jerry Moore (jerry.moore@omes.ok.gov)
2022-10-05 - 8:18:03 PM GMT- IP address: 104.28.97.26

Document e-signed by Jerry Moore (jerry.moore@omes.ok.gov)
Signature Date: 2022-10-05 - 8:18:56 PM GMT - Time Source: server- IP address: 52.71.63.225- Located near: (0.0, 0.0)

Offline document events synchronized and recorded
2022-10-05 - 8:19:02 PM GMT - Time Source: server- IP address: 52.71.63.225

Agreement completed.
2022-10-05 - 8:19:02 PM GMT