Health and Human Services Commission

Purchase Order

Dispatch via Print

Payment Terms	Freight Terms	Ship Via
Net 30	N/A, Service, Pick up, etc.	NONE

If advertised by informal bid, Invitation for Offer, or Request for Proposal; all specifications, terms, and conditions set forth in the advertisement and vendor's conforming responses become a part of this numbered purchase order. Contractor guarantees goods or services delivered meet or exceed numbered purchase order requirements.

All shipments, shipping papers, invoices, and correspondence must be identified with our Purchase Order Number.

Purchase Order **HHSTX-4-0000332988**

Date	Revision	Page
11/10/23		1

Ship To: 1933 - Austin:4616 W Howard Ln
HEALTH & HUMAN SERVICES COMMISSION
4616 W Howard Ln
Ste 840
Austin TX 78728
United States

Vendor: 1522189693 7
CARAHSOFT TECHNOLOGY CORPORATION
11493 SUNSET HILLS RD STE 100
RESTON VA 20190-5230
United States

Bill To: Invoice-HHSC Accounting
HEALTH & HUMAN SERVICES COMMISSION
4601 W Guadalupe St
Austin TX 78751
United States

Fax: 512/424-6901
Email: HHSC_AP@hhsc.state.tx.us

Exempt Reason: N/A

Purchaser: Kozlovsky,Brian M 9036833421, X7112

Line-Sch	Inventory Item ID - Line Description	Class/Item	Quantity	UOM	PO Price	Extended Amt	Due Date

CONFIRMATION ORDER - DO NOT DUPLICATE

(For HHS Accounts Payable Use Only): WIC Program invoice approver: Melissa Anderson (melissa.anderson@hhs.texas.gov)

FY24 Funding
IT/I

PO Service Dates: 11/19/2023 to 11/18/2024

This purchase order is contingent upon the continued availability of lawful appropriations by the Texas Legislature and may be canceled at any time in whole or part without penalty. HHS or the agency does not commit to ordering specific quantities of goods/services or dollar amounts with respect to this purchase order. The agency shall be obligated to pay for only those goods and/or services ordered and received by the agency. Any funds not utilized by 08/31/2024 are automatically canceled.

Purchase order issued in accordance with Texas Government Code §2157.068, and DIR-TSO-4288, DIR-IT Solicitation #0000232753 (reference Quote #38147385).

Vendor: Carahsoft Technology Corporation
Contact: Michelle Gomez-Colon
Phone: 571-662-3354
Email: michelle.gomez-colon@carahsoft.com

Agency Contacts:
Debbie Lehman 512-341-4517 (debbie.lehman@hhs.texas.gov)
Connie Booker 512-341-4524 (connie.booker1@hhs.texas.gov)
Req: 0000232753

HHSC Purchasing Contact: Brian Kozlovsky, CTCD
Phone: 903-683-3421 x7112 Fax: 903-683-7995
Email: brian.kozlovsky@hhs.texas.gov

1-1	Qualtrics CrossXM Bundle, CrossXM, Foundation, Engagement, Part #251-CrossXM-Bundle, Term: 11/19/23 - 11/18/24	208-21	1.00	LOT	877671.49000	$877,671.49	11/30/2023

Schedule Total $877,671.49

Health and Human Services Commission

Purchase Order

Dispatch via Print

Payment Terms	Freight Terms	Ship Via
Net 30	N/A, Service, Pick up, etc.	NONE

If advertised by informal bid, Invitation for Offer, or Request for Proposal; all specifications, terms, and conditions set forth in the advertisement and vendor's conforming responses become a part of this numbered purchase order. Contractor guarantees goods or services delivered meet or exceed numbered purchase order requirements.

All shipments, shipping papers, invoices, and correspondence must be identified with our Purchase Order Number.

Purchase Order **HHSTX-4-0000332988**

Date	Revision	Page
11/10/23		2

Ship To: 1933 - Austin:4616 W Howard Ln
HEALTH & HUMAN SERVICES COMMISSION
4616 W Howard Ln
Ste 840
Austin TX 78728
United States

Vendor: 1522189693 7
CARAHSOFT TECHNOLOGY CORPORATION
11493 SUNSET HILLS RD STE 100
RESTON VA 20190-5230
United States

Bill To: Invoice-HHSC Accounting
HEALTH & HUMAN SERVICES COMMISSION
4601 W Guadalupe St
Austin TX 78751
United States

Fax: 512/424-6901
Email: HHSC_AP@hhsc.state.tx.us

Exempt Reason: N/A

Purchaser: Kozlovsky,Brian M 9036833421, X7112

Line-Sch	Inventory Item ID - Line Description	Class/Item	Quantity	UOM	PO Price	Extended Amt	Due Date
	Includes: DesignXM Enterprise - User: Includes up to 5 SMS Text Reserve: up to 3000000 CrossXM Employees: up to 3000 CX Success Package - Certifications - Engage CX Success Package - XM Expert Coaching - Engage CX Success Package - TAM CX Success Package - Signature Support Location - User: Includes up to 10 Digital - Page Views (Millions): up to 10 Digital - User Foundation - Responses: up to 750000 Foundation - User: Includes up to 2500 Engagement - Employee: up to 3000 Engagement Add-on - Employee: up to 3000 360 Feedback - Employee: up to 600						
					Item Total for Line 1	$877,671.49	
2-1	Qualtrics Short Message Service Credit-50000, Part #251-SMS Credit-50000, Term: 11/19/23 - 11/18/24	208-21	1.00	LOT	29437.80000	$29,437.80	11/30/2023
					Schedule Total	$29,437.80	
					Item Total for Line 2	$29,437.80	
3-1	Qualtrics CX Success Package, XM Expert Coaching, Engage, Part #CX-SUCCESS, Term: 11/19/23 - 11/18/24	208-21	1.00	LOT	31494.85000	$31,494.85	11/30/2023
					Schedule Total	$31,494.85	
					Item Total for Line 3	$31,494.85	
4-1	Qualtrics Custom Implementation - Walker, Part #CUST-IMPL, Term: 11/19/23 - 11/18/24	208-21	1.00	LOT	61391.75000	$61,391.75	11/30/2023

Health and Human Services Commission

Purchase Order

Dispatch via Print

Payment Terms	Freight Terms	Ship Via
Net 30	N/A, Service, Pick up, etc.	NONE

If advertised by informal bid, Invitation for Offer, or Request for Proposal; all specifications, terms, and conditions set forth in the advertisement and vendor's conforming responses become a part of this numbered purchase order. Contractor guarantees goods or services delivered meet or exceed numbered purchase order requirements.

All shipments, shipping papers, invoices, and correspondence must be identified with our Purchase Order Number.

Purchase Order **HHSTX-4-0000332988**

Date	Revision	Page
11/10/23		3

Ship To: 1933 - Austin:4616 W Howard Ln
HEALTH & HUMAN SERVICES COMMISSION
4616 W Howard Ln
Ste 840
Austin TX 78728
United States

Vendor: 1522189693 7
CARAHSOFT TECHNOLOGY CORPORATION
11493 SUNSET HILLS RD STE 100
RESTON VA 20190-5230
United States

Bill To: Invoice-HHSC Accounting
HEALTH & HUMAN SERVICES COMMISSION
4601 W Guadalupe St
Austin TX 78751
United States

Fax: 512/424-6901
Email: HHSC_AP@hhsc.state.tx.us

Exempt Reason: N/A

Purchaser: Kozlovsky,Brian M 9036833421, X7112

Line-Sch	Inventory Item ID - Line Description	Class/Item	Quantity	UOM	PO Price	Extended Amt	Due Date

Schedule Total $61,391.75

Item Total for Line 4 $61,391.75

Total PO Amount $999,995.89

No substitutions or cancellations are permitted without prior approval by Health & Human Services Commission. If contractor fails to deliver by promised delivery date (or reasonable time thereafter) or fails to meet requirements, Health & Human Services Commission reserves the right to purchase elsewhere and charge an increased cost and handling to contractor.

Over shipments will not be accepted unless authorized by Buyer prior to shipment. The dispute resolution process provided for in Chapter 2260 of the Texas Government Code must be used by the Health & Human Services Commission and Contractor to attempt to resolve all disputes arising under the contract.

Performance under this purchase order is acceptance of the attached affirmations and terms and conditions.

Authorized By

Brian Kozlovsky, CTCD

11/21/2023

HEALTH AND HUMAN SERVICES COMMISSION
UNIFORM TERMS AND CONDITIONS AND AFFIRMATIONS
FOR PRICE REQUESTS UNDER DIR COOPERATIVE CONTRACTS (HHS OCC Version 1, 3-01-23)

1. PRICE REQUEST (PR)

1.1 In accordance with Section 2157.068(e-1) of the Texas Government Code, the Price Request (PR) is being issued to vendors that provide commodity items under Department of Information Resources (DIR) Contracts.

1.2 The Texas Health and Human Services (HHS) System is comprised of more than 41,000 public servants under two agencies: the Health and Human Services Commission (HHSC) and the Department of State Health Services (DSHS). HHSC and DSHS are each a System Agency (Agency) with independent procurement authority. Unless DSHS is specified as the ordering agency in the specifications or purchase order, HHSC is the ordering agency.

2. RESPONSE REQUIREMENTS

2.1 By submitting a Response, Respondent agrees to comply with all terms of the Price Request (PR) issued by Agency.

2.2 In its Response, Respondent must specify the DIR Contract under which the Response is submitted.

2.3 Respondent must price per unit shown. Unit prices shall govern in the event of extension errors.

2.4 Respondent pricing is firm for Agency acceptance for ninety (90) calendar days from Response due date.

2.5 If an early payment discount is available to Agency, then Respondent in its Response must describe with specificity the early payment discount offered and the discount percentage that would apply to early payment within ten, fifteen, twenty, or twenty-five calendar days after receipt of a correct invoice.

2.6 Respondent acknowledges that the contract is not exclusive, and that Agency may solicit the same or similar commodity items from other service providers at any time.

2.7 Agency makes no guarantee of volume or usage of work under the contract.

2.8 Respondent is responsible for all expenses related to the preparation and submission of its Response.

2.9 A Response that is late, illegible, incomplete, or otherwise non-responsive will not be considered. If the Response is submitted electronically, Agency shall not be responsible for failure of electronic equipment or operator error.

2.10 A Response that does not meet all of the requirements or contain all of the required documentation specified in the PR may be rejected as non-responsive.

3. IT COMMODITY REQUIREMENTS

3.1 Unless otherwise indicated in the specifications, the commodity item(s) shall be new and unused and of current production.

3.2 All electrical items must meet all applicable OSHA standards and regulations, and bear the appropriate listing from UL, FMRC or NEMA.

3.3 Manufacturer's standard warranty shall apply unless otherwise stated in the specifications or Respondent's DIR Contract.

3.4 Respondent will use commercially reasonable efforts to perform services in a timely manner and devote adequate resources to meet its obligations under the contract.

3.5 Respondent will convey to Agency clear title, ownership and licenses, whichever is applicable, to each commodity item provided under the contract.

3.6 For each software product, Respondent represents that it has sufficient right, title, and interest in the software to grant the license required by the contract.

3.7 If Respondent is a software publisher, Respondent represents that the software does not infringe upon or constitute a misuse or misappropriation of any patent, trademark, copyright, trade secret or other proprietary right.

3.8 Respondent represents that the software and equipment provided under the contract will have the functionality specified in the associated technical documentation.

3.9 For a Respondent hosted service, Respondent shall, unless otherwise specified in the specifications or contract, provide to Agency for no additional compensation all Agency Data in a commercially standard database export format within thirty (30) calendar days following the date of contract expiration or termination.

3.10 In accordance with 45 C.F.R. 95.617, Respondent will provide requisite ownership rights in software or modifications thereof and associated documentation designed, developed or installed with Federal financial participation.

3.11 For purposes of a contract for software where HHSC is the ordering agency, HHSC is the licensee. HHSC, as authorized by applicable statute, provides administrative support to certain state agencies. For the avoidance of doubt, HHSC's internal business use of software includes any activities consistent with HHSC's statutory authority and such activities shall not be construed to be a service bureau, application service provider, provider of services to third parties, distribution outside of HHSC's organization, or similar activity. Respondent

acknowledges and agrees that HHSC's internal business use is within the scope of the license granted in the contract.

3.12 During the contract term, Agency may be presented with the requirement to "agree" to a click through agreement before accessing software provided under the contract. Respondent expressly agrees that the terms of any such click through agreement shall be considered null and void and shall not apply in any manner to Agency. For the avoidance of doubt, the terms of the contract supersede any clickwrap, shrinkwrap, browsewrap, terms of service, or similar agreement which may accompany the software.

3.13 Any software deployment verification activities conducted by Respondent will be (i) not more often than once each year, unless Respondent has a reasonable basis to believe that a violation of the license terms has occurred, (ii) in a manner that minimizes disruption to Agency's business operations, and (iii) during Agency's normal business hours. Respondent will comply with applicable Agency confidentiality requirements as well as information security, building access, and health and safety policies and procedures. Respondent, at its sole expense, may use an independent auditor to assist with such verification, provided Respondent has a written confidentiality agreement in place with such auditor that is no less stringent than the confidentiality obligations set forth in the contract. Respondent will provide written notice if any verification activity indicates that Agency has used any software in excess of Agency's use authorizations or Agency is otherwise not in compliance with the license terms. Respondent will afford Agency at least thirty (30) days to review the findings, correct any factual errors, and annotate the findings with Agency's position as part of Respondent's verification activities. In the event that a non-compliance determination is made, Respondent shall submit an invoice for any overuse of the software to Agency under Chapter 2251 of the Texas Government Code at rates provided to public sector entities, provided such rates do not exceed retail prices. Respondent understands that Agency will comply with applicable state procurement law in the acquisition of additional licenses subject to this section.

4. AWARD OF CONTRACT

4.1 A Respondent's Response to the PR is an offer to contract based upon the terms, conditions and specifications contained herein. A Response does not become binding and enforceable until accepted by the Agency, followed by issuance of a purchase order to Respondent to award the contract.

4.2 Agency reserves the right to accept or reject all or any part of the Response, waive minor technicalities, and award the contract to best serve the interests of the State.

4.3 No terms or conditions advanced by Respondent, by way of exception, assumption or other means, are included as part of the contract unless expressly agreed in writing by Agency.

4.4 Except as otherwise provided in the negotiated terms and conditions, if any, that are expressly identified as such in a formal signed agreement or the purchase order resulting from the PR, the entire contract between Agency and successful Respondent shall consist of the following documents: (1) the purchase order and purchase order change notices; (2) the PR; (3) the successful Respondent's DIR Contract, (4) successful Respondent's Response, and (5) if applicable, a formal signed agreement. Except as otherwise provided in the negotiated terms and conditions, if any, that are expressly identified as such in the formal signed agreement or purchase order resulting from the PR, in the event of conflicting terms or provisions in the contract, the PR and the purchase order and the purchase order change notices, if any, will control.

5. DELIVERY

5.1 No substitutions are permitted without written approval of Agency.

5.2 Delivery shall be made during normal working hours only, unless prior approval has been obtained from Agency.

5.3 If delivery will be delayed, Respondent must notify Agency. Default in promised delivery or failure to meet specifications authorizes Agency to purchase the commodity items elsewhere, pursue financial remedies available under Respondent's DIR Contract, and terminate the contract for cause.

5.4 A commodity item that is delivered and fails to meet specifications or is not the actual item awarded on the contract shall be rejected and may be returned at Respondent's expense.

6. PAYMENT, INVOICING, DISCOUNTS

6.1 Chapter 2251 of the Texas Government Code shall govern remittance of payment and remedies for late payment and non-payment.

6.2 An itemized invoice must be submitted showing order number to the address indicated on the purchase order.

6.3 If Respondent at any time during the term of the contract provides a discount on the contract costs, Respondent will notify Agency in writing at least ten (10) calendar days prior to effective date of discount. Agency will generate a purchase order change notice and send a revised purchase order to Respondent.

6.4 Reimbursement for travel, meals, lodging or other related expenses shall not be made unless specifically provided for in the contract. When the reimbursement of travel expenses is authorized by the contract and approved in writing by the Agency, all such expenses will be reimbursed in accordance with the rates set by the State of Texas *Textravel* available at the Texas Comptroller of Public Accounts State Travel Management Program website.

6.5 Agency shall pay no costs or other amounts incurred by any entity in responding to the PR or incurred prior to the effective date of the contract.

6.6 Purchases made for State of Texas use are exempt from the State Sales Tax and Federal Excise Tax. Tax Exemption Certificates will be furnished upon written request.

7. LEGAL NOTICES

7.1 Respondent shall send legal notices to the applicable Agency at the address below and provide a copy to the Agency Contract Representative identified in the contract:

To HHSC:

Health and Human Services Commission
Attn: Office of Chief Counsel
4601 W. Guadalupe Street, MC-1100
Austin, Texas 78751

To DSHS:

Department of State Health Services
Attn: Office of General Counsel
1100 West 49th Street, MC-1919
Austin, Texas 78714

With Copy To:
Health and Human Services Commission
Attn: Office of Chief Counsel
4601 W. Guadalupe Street, MC-1100
Austin, Texas 78751

7.2 Agency may change the designated notice address in Section 7.1 by written notice to Respondent.

7.3 Legal notices given by Respondent to Agency may be deposited in the United States mail or sent by common carrier, and such notices shall be deemed delivered when received by Agency.

7.4 Agency shall send legal notices to Respondent's representative in accordance with the provisions of Respondent's DIR Contract.

8. TEXAS REQUIRED CONTRACT CLAUSES

8.1 General. The terms in this Section 8 are required by Section 2262.051(d)(1) of the Texas Government Code. In the event of conflict or inconsistency between a term in this Section 8 and a term in Respondent's DIR Contract, the term of the DIR Contract supersedes and controls.

8.2 Antitrust Affirmation. Respondent represents and warrants that, in accordance with Section 2155.005 of the Texas Government Code, neither Respondent nor the firm, corporation, partnership, or institution represented by Respondent, or anyone acting for such a firm, corporation or institution has (1) violated any provision of the Texas Free Enterprise and Antitrust Act of 1983, Chapter 15 of the Texas Business and Commerce Code, or the federal antitrust laws, or (2) communicated directly or indirectly the contents of the Response to any competitor or any other person engaged in the same line of business as Respondent.

8.3 Assignment by Respondent. In accordance with Section 2262.056 of the Texas Government Code, Respondent may not assign the contract or assign, transfer or delegate, in whole or in part, any of its interest in, or rights or obligations under, the contract without the prior written consent of Agency, and any attempted or purported assignment, transfer or delegation thereof without such consent shall be null and void.

8.4 Buy Texas Affirmation. Respondent agrees to comply with Section 2155.4441 of the Texas Government Code, relating to use of service contracts and the purchase of products and materials produced in the State of Texas.

8.5 Child Support Obligation Affirmation. Under Section 231.006 of the Family Code, Respondent certifies that the individual or business entity named in the contract, bid or application is not ineligible to receive the specified grant, loan, or payment and acknowledges that the contract may be terminated and payment may be withheld if this certification is inaccurate. If the certification is shown to be false, Respondent may be liable for additional costs and damages set out in Section 231.006(f) of the Family Code.

8.6 Cloud Computing State Risk and Authorization Management Program. Pursuant to Section 2054.0593(d)-(f) of the Texas Government Code, relating to cloud computing state risk and authorization management program, Respondent represents and warrants that it complies with the requirements of the state risk and authorization management program and Respondent agrees that throughout the term of the contract it shall maintain its certifications and comply with the program requirements in the performance of the contract.

8.7 Computer Equipment Recycling Program. If Respondent is submitting a Response for the purchase or lease of computer equipment, then Respondent certifies that it is in compliance with Subchapter Y, Chapter 361 of the Texas Health and Safety Code related to the Computer Equipment Recycling Program and the Texas Commission on Environmental Quality rules in 30 TAC Chapter 328.

8.8 Contracting Information Responsibilities. Respondent represents and warrants that it will comply with the requirements of Section 552.372(a) of the Texas Government Code. Except as provided by Section 552.374(c) of the Texas Government Code, the requirements of Subchapter J, Chapter 552 of the Government Code, may apply to the contract and Respondent agrees that the contract can be terminated if Respondent knowingly or intentionally fails to comply with a requirement of that subchapter.

8.9 COVID-19 Vaccine Passport Prohibition. Under Section 161.0085 of the Texas Health and Safety Code, Respondent certifies that the individual or business entity named in the Response or contract is not ineligible to receive the specified contract.

8.10 Critical Infrastructure Affirmation. Pursuant to Government Code Section 2274.0102, Respondent certifies that neither it nor its parent company, nor any affiliate of Respondent or its parent company, is: (1) majority owned or controlled by citizens or governmental entities of China, Iran, North Korea, Russia, or any other country designated by the Governor under Government Code Section 2274.0103, or (2) headquartered in any of those countries.

8.11 Cybersecurity Training. If Respondent has access to any state computer system or database, Respondent shall complete cybersecurity training and verify completion of the training program to Agency pursuant to and in accordance with Section 2054.5192 of the Government Code.

8.12 Data Management and Security Controls. In accordance with Section 2054.138 of the Texas Government Code, Respondent certifies that it will comply with the security controls required under the contract and will maintain records and make them available to Agency as evidence of Respondent's compliance with the required controls.

8.13 Dealings with Public Servants Affirmation. Respondent has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with the submitted Response.

8.14 Debts and Delinquencies Affirmation. Respondent acknowledges and agrees that, to the extent Respondent owes any debt including, but not limited to, delinquent taxes, delinquent student loans, and child support owed to the State of Texas, any payments or other amounts Respondent is otherwise owed under the contract may be applied toward any debt Respondent owes the State of Texas until the debt is paid in full. These provisions are effective at any time Respondent owes any such debt or delinquency.

8.15 Disaster Recovery Plan. Upon request of Agency, Respondent shall provide the descriptions of its business continuity and disaster recovery plans.

8.16 Dispute Resolution. Disputes arising under the contract shall be resolved in accordance with the dispute resolution process provided in Chapter 2260 of the Texas Government Code.

8.17 Energy Company Boycotts. If Respondent is required to make a verification pursuant to Section 2274.002 of the Texas Government Code, Respondent verifies that Respondent does not boycott energy companies and will not boycott energy companies during the term of the contract. If Respondent does not make that verification, Respondent must so indicate in its Response and state why the verification is not required.

8.18 Entities that Boycott Israel. If Respondent is required to make a certification pursuant to Section 2271.001 of the Texas Government Code, Respondent certifies that Respondent does not boycott Israel and will not boycott Israel during the term of the contract. If Respondent does not make that certification, Respondent must indicate that in its Response and state why the certification is not required.

8.19 E-Verify Program. Respondent certifies that for contracts for services, Respondent shall utilize the U.S. Department of Homeland Security's E-Verify system during the term of the contract to determine the eligibility of:

a. all persons employed by Respondent to perform duties within Texas; and
b. all persons, including subcontractors, assigned by Respondent to perform work pursuant to the contract within the United States of America.

8.20 Excess Obligations Prohibited. The contract shall not be construed as creating a debt on behalf of Agency in violation of Article III, Section 49a of the Texas Constitution. Respondent understands that all obligations of Agency under the contract are subject to the availability of state funds. If such funds are not appropriated or become unavailable, the contract may be terminated by Agency.

8.21 Excluded Parties. Respondent certifies that it is not listed in the prohibited vendors list authorized by Executive Order No. 13224, *"Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism"*, published by the United States Department of the Treasury, Office of Foreign Assets Control.

8.22 Executive Head of a State Agency Affirmation. Under Section 669.003 of the Texas Government Code, relating to contracting with an executive head of a state agency, Respondent represents that no person who served as an executive of Agency, in the past four (4) years, was involved with or has any interest in the contract. If Respondent employs or has used the services of a former executive of Agency, then Respondent shall provide the following information in the Response: name of the former executive, the name of the state agency, the date of separation from the state agency, the position held with Respondent, and the date of employment with Respondent.

8.23 False Statements. If Respondent signs the Response with a false statement or it is subsequently determined that Respondent has violated any of the representations, warranties, guarantees, certifications, or affirmations included in the Response, Respondent will be in default under the contract and Agency may terminate or void the contract.

8.24 Financial Participation Prohibited Affirmation. Pursuant to Section 2155.004(a) of the Texas Government Code, Respondent certifies that neither Respondent nor any person or entity represented by Respondent has received compensation from Agency to participate in the preparation of the specifications or solicitation on which the Response or contract is based. Under Section 2155.004(b) of the Texas Government Code, Respondent certifies that the individual or business entity named in the Response or contract is not ineligible to receive the specified contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate.

8.25 Firearm Entities and Trade Associations Discrimination. If Respondent is required to make a verification pursuant to Section 2274.002 of the Texas Government Code, Respondent verifies that it (1) does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and (2) will not discriminate during the term of the contract against a firearm entity or firearm trade association. If Respondent does not make that verification, Respondent must so indicate in its Response and state why the verification is not required.

8.26 Foreign Terrorist Organizations. Section 2252.152 of the Texas Government Code prohibits Agency from awarding a contract to any person who does business with Iran, Sudan, or a foreign terrorist organization as defined in Section 2252.151 of the Texas Government Code. Respondent certifies that it is not ineligible to receive the contract.

8.27 Governing Law and Venue. The contract shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the contract is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to the contracting Agency.

8.28 Human Trafficking Prohibition. Under Section 2155.0061 of the Texas Government Code, the Respondent certifies that the individual or business entity named in the Response or contract is not ineligible to receive the specified contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate.

8.29 Indemnification (General). **RESPONDENT SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS THE STATE OF TEXAS AND AGENCY, AND THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, AND DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF, OR RESULTING FROM ANY ACTS, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF, OR RESULTING FROM ANY ACTS OR OMISSIONS OF RESPONDENT OR ITS AGENTS, EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR PERFORMANCE OF THE CONTRACT AND ANY PURCHASE ORDERS ISSUED UNDER THE CONTRACT. THE DEFENSE SHALL BE COORDINATED BY RESPONDENT WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND RESPONDENT MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM THE OFFICE OF THE TEXAS ATTORNEY GENERAL. RESPONDENT AND AGENCY AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM.**

8.30 Indemnification (IP). **RESPONDENT SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS AGENCY AND THE STATE OF TEXAS FROM AND AGAINST ANY AND ALL CLAIMS, VIOLATIONS, MISAPPROPRIATIONS OR INFRINGEMENT OF ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHTS AND/OR OTHER INTANGIBLE PROPERTY, PUBLICITY OR PRIVACY RIGHTS, AND/OR IN CONNECTION WITH OR ARISING FROM: (1) THE PERFORMANCE OR ACTIONS OF RESPONDENT PURSUANT TO THE CONTRACT; (2) ANY DELIVERABLE, WORK PRODUCT, CONFIGURED SERVICE OR OTHER SERVICE PROVIDED HEREUNDER; AND/OR (3) AGENCY'S AND/OR RESPONDENT'S USE OF OR ACQUISITION OF ANY REQUESTED SERVICES OR OTHER ITEMS PROVIDED TO AGENCY BY RESPONDENT OR OTHERWISE TO WHICH AGENCY HAS ACCESS AS A RESULT OF RESPONDENT'S PERFORMANCE UNDER THE CONTRACT. RESPONDENT AND AGENCY AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM. RESPONDENT SHALL BE LIABLE TO PAY ALL COSTS OF DEFENSE, INCLUDING ATTORNEYS' FEES. THE DEFENSE SHALL BE COORDINATED BY RESPONDENT WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL (OAG) WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND RESPONDENT MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM OAG. IN ADDITION, RESPONDENT WILL REIMBURSE AGENCY AND THE STATE OF TEXAS FOR ANY CLAIMS, DAMAGES, COSTS, EXPENSES OR OTHER AMOUNTS, INCLUDING, BUT NOT LIMITED TO, ATTORNEYS' FEES AND COURT COSTS, ARISING FROM ANY SUCH CLAIM. IF AGENCY DETERMINES THAT A CONFLICT EXISTS BETWEEN ITS INTERESTS AND THOSE OF RESPONDENT OR IF AGENCY IS REQUIRED BY APPLICABLE LAW TO SELECT SEPARATE COUNSEL, AGENCY WILL BE PERMITTED TO**

SELECT SEPARATE COUNSEL AND RESPONDENT WILL PAY ALL REASONABLE COSTS OF AGENCY'S COUNSEL.

8.31 National Anthem Verification. Respondent will play the United States national anthem at the beginning of each team sporting event held at the Respondent's home venue or other venue controlled by Respondent for the event. Failure to comply with this obligation constitutes a default of the contract, and immediately subjects Respondent to the penalties for default, such as repayment of money received or ineligibility for additional money. In addition, Respondent may be debarred from contracting with the State. Agency or the Attorney General may strictly enforce this provision.

8.32 No Conflicts of Interest. Respondent represents and warrants that the provision of goods and services or other performance under the contract will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.

8.33 Prior Disaster Relief Contract Violation. Under Sections 2155.006 and 2261.053 of the Texas Government Code, Respondent certifies that the individual or business entity named in the Response or contract is not ineligible to receive the specified contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate.

8.34 Public Information Act. Respondent understands that Agency will comply with the Texas Public Information Act (Chapter 552 of the Texas Government Code) as interpreted by judicial rulings and opinions of the Attorney General of the State of Texas. Information, documentation, and other material in connection with the PR or any resulting contract may be subject to public disclosure pursuant to the Texas Public Information Act. In accordance with Section 2252.907 of the Texas Government Code, Respondent is required to make any information created or exchanged with the State pursuant to the contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.

8.35 Signature Authority. By submitting the Response, Respondent represents and warrants that the individual submitting this document and the documents made part of the Response is authorized to sign such documents on behalf of the Respondent and to bind the Respondent under any contract that may result from the submission of the Response.

8.36 State Auditor's Right to Audit. The state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under the contract or indirectly through a subcontract under the contract. The acceptance of funds directly under the contract or indirectly through a subcontract under the contract acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit.

8.37 Suspension and Debarment. Respondent certifies that it and its principals are not suspended or debarred from doing business with the state or federal government as listed on the *State of Texas Debarred Vendor List* maintained by the Texas Comptroller of Public Accounts and the *System for Award Management (SAM)* maintained by the General Services Administration.

8.38 Television Equipment Recycling Program. If Respondent is submitting a Response for the purchase or lease of covered television equipment, then Respondent certifies that it is compliant with Subchapter Z, Chapter 361 of the Texas Health and Safety Code related to the Television Equipment Recycling Program.

8.39 Terms and Conditions Attached to Response. Any terms and conditions attached to a Response will not be considered unless specifically referred to in the Response.

9. HHSC REQUIRED CONTRACT CLAUSES

9.1 Abortion Funding Limitation**.** Respondent understands, acknowledges, and agrees that, pursuant to Article IX of the General Appropriations Act (the Act), to the extent allowed by federal and state law, money appropriated by the Texas Legislature may not be distributed to any individual or entity that, during the period for which funds are appropriated under the Act:

a. performs an abortion procedure that is not reimbursable under the state's Medicaid program;
b. is commonly owned, managed, or controlled by an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program; or
c. is a franchise or affiliate of an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program.

The provision does not apply to a hospital licensed under Chapter 241, Health and Safety Code, or an office exempt under Section 245.004(2), Health and Safety Code. Respondent represents and warrants that it is not ineligible, nor will it be ineligible during the term of the contract, to receive appropriated funding pursuant to Article IX.

9.2 Funding Eligibility. Respondent understands, acknowledges, and agrees that, pursuant to Chapter 2272 (eff. Sept. 1, 2021, Ch. 2273) of the Texas Government Code, except as exempted under that Chapter, HHSC cannot contract with an abortion provider or an affiliate of an abortion provider. Contractor certifies that it is not ineligible to contract with HHSC under the terms of Chapter 2272 (eff.

Sept. 1, 2021, Ch. 2273) of the Texas Government Code.

9.3 Prohibition on Abortions**.** Respondent understands, acknowledges, and agrees that, pursuant to Article II of the General Appropriations Act, (1) no funds shall be used to pay the direct or indirect costs (including marketing, overhead, rent, phones, and utilities) of abortion procedures provided by contractors of HHSC; and (2) no funds appropriated for Medicaid Family Planning, Healthy Texas Women Program, or the Family Planning Program shall be distributed to individuals or entities that perform elective abortion procedures or that contract with or provide funds to individuals or entities for the performance of elective abortion procedures. Respondent represents and warrants that it is not ineligible, nor will it be ineligible during the term of the contract, to receive appropriated funding pursuant to Article II.

9.4 Enterprise Information Management Standards. Respondent shall conform to HHS standards for data management as described by the policies of the HHS Office of Data, Analytics, and Performance. These include, but are not limited to, standards for documentation and communication of data models, metadata, and other data definition methods that are required by HHS for ongoing data governance, strategic portfolio analysis, interoperability planning, and valuation of HHS System data assets.

9.5 Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment (2 CFR 200.216)**.** Respondent certifies that the individual or business entity named in the Response or contract is not ineligible to receive the specified contract or funding pursuant to 2 C.F.R. 200.216.

9.6 Enforcement of Certain Federal Firearms Laws Prohibited. In accordance with House Bill 957, Acts 2021, 87th Leg., R.S., if Texas Government Code, Section 2.101 is applicable to Respondent, Respondent certifies that it is not ineligible to receive state grant funds pursuant to Texas Government Code, Section 2.103.

9.7 Civil Rights.

a. Respondent agrees to comply with state and federal anti-discrimination laws, including:
   - Title VI of the Civil Rights Act of 1964 (42 U.S.C. §2000d et seq.);
   - Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. §794);
   - Americans with Disabilities Act of 1990 (42 U.S.C. §12101 et seq.);
   - Age Discrimination Act of 1975 (42 U.S.C. §§6101-6107);
   - Title IX of the Education Amendments of 1972 (20 U.S.C. §§1681-1688);
   - Food and Nutrition Act of 2008 (7 U.S.C. §2011 et seq.); and
   - The Agency's administrative rules, as set forth in the Texas Administrative Code, to the extent applicable to the contract.

b. Respondent agrees to comply with all amendments to the above-referenced laws, and all requirements imposed by the regulations issued pursuant to these laws. These laws provide in part that no persons in the United States may, on the grounds of race, color, national origin, sex, age, disability, political beliefs, or religion, be excluded from participation in or denied any aid, care, service or other benefits provided by Federal or State funding, or otherwise be subjected to discrimination.

c. Respondent agrees to comply with Title VI of the Civil Rights Act of 1964, and its implementing regulations at 45 C.F.R. Part 80 or 7 C.F.R. Part 15, prohibiting a contractor from adopting and implementing policies and procedures that exclude or have the effect of excluding or limiting the participation of clients in its programs, benefits, or activities on the basis of national origin. State and federal civil rights laws require contractors to provide alternative methods for ensuring access to services for applicants and recipients who cannot express themselves fluently in English. Respondent agrees to take reasonable steps to provide services and information, both orally and in writing, in appropriate languages other than English, in order to ensure that persons with limited English proficiency are effectively informed and can have meaningful access to programs, benefits, and activities.

d. Respondent agrees to post applicable civil rights posters in areas open to the public informing clients of their civil rights and including contact information for the HHS Civil Rights Office. The posters are available on the HHS website at: https://hhs.texas.gov/about-hhs/your-rights/civil-rights-office/civil-rights-posters.

e. Respondent agrees to comply with Executive Order 13279, and its implementing regulations at 45 C.F.R. Part 87 or 7 C.F.R. Part 16. These provide in part that any organization that participates in programs funded by direct financial assistance from the United States Department of Agriculture or the United States Department of Health and Human Services shall not discriminate against a program beneficiary or prospective program beneficiary on the basis of religion or religious belief.

f. Upon request, Respondent shall provide HHSC's Civil Rights Office with copies of the Respondent's civil rights policies and procedures.

g. Respondent must notify HHSC's Civil Rights Office of any complaints of discrimination received relating to its performance under the contract. This notice must be delivered no more than ten (10) calendar days after receipt of a complaint. Notice provided pursuant to this section must be directed to:
   HHSC Civil Rights Office
   701 W. 51st Street, Mail CodeW206
   Austin, Texas 78751
   Phone Toll Free: (888) 388-6332
   Phone: (512) 438-4313
   Fax: (512) 438-5885
   Email: HHSCivilRightsOffice@hhsc.state.tx.us

10. GENERAL TERMS

10.1 DIR Contract Terms. The terms and conditions of the PR may not weaken or diminish any terms and conditions of the Respondent's DIR Contract. To the extent that the DIR Contract provides more favorable terms to Agency or imposes more rigorous obligations on Respondent, the DIR Contract terms supersede and control over the PR. As permitted by the DIR Contract, Agency may add additional terms and negotiate written agreements regarding statements of work, service level agreements, remedies, acceptance criteria, information confidentiality and security requirements, and other terms specific to the contract.

10.2 Confidentiality. Respondent shall maintain as confidential and shall not disclose to third parties without Agency's prior written consent, any Agency information including but not limited to Agency Data, Agency's business activities, practices, systems, conditions and services. This section will survive termination or expiration of the contract. The obligations of Respondent under this section will survive termination or expiration of the contract. This requirement must be included in all subcontracts awarded by Respondent.

10.3 Agency Data.

a. As between Agency and Respondent, all data and information acquired, accessed, or made available to Respondent by, through, or on behalf of Agency or Agency contractors, including all electronic data generated, processed, transmitted, or stored by Respondent in the course of providing data processing services in connection with Respondent's performance hereunder (the "Agency Data"), is owned solely by Agency.

b. Respondent has no right or license to use, analyze, aggregate, transmit, create derivatives of, copy, disclose, or process Agency Data except as required for Respondent to fulfill its obligations under the contract or as authorized in advance in writing by Agency.

c. For the avoidance of doubt, Respondent is expressly prohibited from using, and from permitting any third party to use, Agency Data for marketing, research, or other non-governmental or commercial purposes, without the prior written consent of Agency.

d. Respondent shall make Agency Data available to Agency, including to Agency's designated vendors, as directed in writing by Agency. The foregoing shall be at no cost to Agency.

e. Furthermore, the proprietary nature of Respondent's systems that process, store, collect, and/or transmit Agency Data shall not excuse Respondent's performance of its obligations hereunder.

10.4 Agency Confidential Information Remains Within United States. Respondent shall ensure that all Agency Confidential Information, including such information residing on back-up systems, remains and is stored, processed, accessed, viewed, transmitted, and received, always and exclusively within the contiguous United States.

10.5 Use of State Property.

a. Respondent is prohibited from using State Property for any purpose other than performing services authorized under the contract.

b. State Property includes, but is not limited to, Agency's office space, identification badges, Agency information technology equipment and networks (*e.g.,* laptops, portable printers, cell phones, iPads or tablets, external hard drives, data storage devices, any Agency-issued software, and Agency Virtual Private Network (VPN client)), and any other resources of Agency.

c. Respondent shall not remove State Property from the contiguous United States. In addition, Respondent may not use any computing device to access Agency's network or e-mail while outside of the contiguous United States.

d. Respondent shall not perform any maintenance services on State Property unless the contract expressly authorizes such services.

e. During the time that State Property is in the possession of Respondent, Respondent shall be responsible for: (1) all repair and replacement charges incurred by Agency that are associated with loss of State Property or damage beyond normal wear and tear, and (2) all charges attributable to Respondent's use of State Property that exceeds the contract scope. Respondent shall fully reimburse such charges to Agency within ten (10) calendar days of Respondent's receipt of Agency's notice of amount due. Use of State Property for a purpose not authorized by the contract shall constitute breach of contract and may result in termination of the contract and the pursuit of other remedies available to Agency under contract, at law, or in equity.

10.6 Agency's Right to Audit. Respondent shall make available at reasonable times and upon reasonable notice, and for reasonable periods, work papers, reports, books, records, supporting documents kept current by Respondent pertaining to the contract for purposes of inspecting, monitoring, auditing, or evaluating by Agency and the State of Texas.

10.7 Record Maintenance and Retention.

a. Respondent shall keep and maintain under GAAP or GASB, as applicable, full, true, and complete records necessary to fully disclose to Agency, the Texas State Auditor's Office, the United States Government, and their authorized representatives sufficient information to determine compliance with the terms and conditions of the contract and all state and federal rules, regulations, and statutes.

b. Respondent shall maintain and retain legible copies of the contract and all records relating to the performance of the contract including supporting fiscal documents adequate to ensure that claims for contract funds are in accordance with applicable State of Texas requirements. These records shall be maintained and retained by Respondent for a minimum of seven (7) years after the contract expiration date or seven (7) years after the completion of all audit, claim, litigation, or dispute matters involving the contract are resolved, whichever is later.

10.8 Independent Contractor. Respondent and Respondent's employees, representatives, agents, subcontractors, suppliers, and third-party service providers shall serve as independent contractors in providing the services under the contract. Neither Respondent nor Agency is an agent of the other and neither may make any commitments on the other party's behalf. Respondent shall have no claim against Agency for vacation pay, sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee benefits of any kind. The contract shall not create any joint venture, partnership, agency, or employment relationship between Respondent and Agency.

10.9 Limitation on Authority. Respondent shall not have any authority to act for or on behalf of Agency or the State of Texas except as expressly provided for in the contract; no other authority, power, or use is granted or implied. Respondent may not incur any debt, obligation, expense, or liability of any kind on behalf of Agency or the State of Texas.

10.10 No. Felony Criminal Convictions. Respondent represents that neither Respondent nor any of its employees, agents, or representatives, including any subcontractors and employees, agents, or representative of such subcontractors, have been convicted of a felony criminal offense or that if such a conviction has occurred Respondent has fully advised Agency in writing of the facts and circumstances surrounding the conviction(s).

10.11 No Public Announcements or Marketing Activities. Respondent shall not use Agency's name, logo, or other likeness in any press release, marketing material, or other announcement without Agency's prior written approval. Agency does not endorse any vendor, commodity, or service. Respondent is not authorized to make or participate in any media releases, public announcements, or marketing activities pertaining to the contract or the services to which they relate without Agency's prior written consent, and then only in accordance with explicit written instruction from Agency. The foregoing prohibition includes, without limitation, the placement of banners, pop-up ads, or other advertisements promoting Respondent's or a third party's products, services, workshops, trainings, or other commercial offerings on any website portal or internet-based service or software application hosted or managed by Respondent under the contract.

10.12 Safety Standards. Respondent, its employees, subcontractors, and agents shall observe all safety measures and proper operating procedures at Agency sites at all times. Respondent shall direct its employees, subcontractors, and agents to immediately report to HHSC any defect or unsafe condition encountered while on Agency premises.

10.13 Disaster Recovery Test Plan. Upon request of Agency, Respondent shall provide a copy of its most current disaster recovery test plan.

10.14 Rolling Estoppel. If Respondent is aware a problem exists and fails to report the problem to Agency, Respondent continues to be responsible for meeting the timelines and due dates established in the contract. Under these circumstances, Agency will not be liable for any detrimental consequences.

10.15 Assignment by Agency. Upon written notice, Agency may assign its interest in or duties or rights under the contract without prior written approval to another state agency as designated by the Texas Legislature.

10.16 No Agency Indemnification. **ANY REQUIREMENT THAT AGENCY DEFEND, INDEMNIFY, OR HOLD HARMLESS THE RESPONDENT OR OTHER ENTITY IS HEREBY DELETED FROM THE RESPONSE AND RESPONDENT DOCUMENTS.**

10.17 Termination by Non-Appropriation. In the event the contract is terminated due to non-appropriation of funds, such termination shall not affect Agency's right to use previously paid licensed software through the term of each such license and any maintenance and support paid prior to such termination.

10.18 No Waiver. The failure of Agency to object to or to take affirmative action with respect to any conduct of Respondent which is in violation or breach of the terms of the contract shall not be construed as a waiver of the violation or breach, or of any future violation or breach.

10.19 Sovereign Immunity. Nothing in the contract shall be construed as a waiver of Agency's or the State's sovereign immunity. The contract shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to Agency or the State of Texas.

10.20 Survival of Terms. Expiration or termination of the contract for any reason does not release Respondent from any liability or obligation set forth in the contract that is expressly stated to survive any such expiration or termination, that by its nature would be intended to be applicable following any such expiration or termination, or that is necessary to fulfill the essential purpose of the contract, including without limitation the provisions regarding warranty, indemnification, confidentiality, and rights and remedies upon termination.

DATA USE AGREEMENT
BETWEEN THE
TEXAS HEALTH AND HUMAN SERVICES SYSTEM
AND
CONTRACTOR

This Data Use Agreement ("DUA") is effective as of the date of the Base Contract into which it is incorporated ("Effective Date"), by and between the Texas Health and Human Services System, which includes the Texas Health and Human Services Commission and the Department of State Health Services ("HHS") and Contractor (the "Base Contract").

ARTICLE 1. PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure or transmission of Confidential Information with Contractor, and describe Contractor's rights and obligations with respect to the Confidential Information and the limited purposes for which the Contractor may create, receive, maintain, use, disclose or have access to Confidential Information. This DUA also describes HHS's remedies in the event of Contractor's noncompliance with its obligations under this DUA. This DUA applies to both HHS business associates, as "business associate" is defined in the Health Insurance Portability and Accountability Act (HIPAA), and contractors who are not business associates, who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of HHS, its programs or clients as described in the Base Contract. As a best practice, HHS requires its contractors to comply with the terms of this DUA to safeguard all types of Confidential Information.

As of the Effective Date of this DUA, if any provision of the Base Contract conflicts with this DUA, this DUA controls.

ARTICLE 2. DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the following meanings:

"Authorized Purpose" means the specific purpose or purposes described in the Base Contract for Contractor to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

"Authorized User" means a person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom Contractor warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

"Breach" means an impermissible use or disclosure of electronic or non-electronic sensitive personal information by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of Confidential Information such that the use or disclosure poses a risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Any acquisition, access, use, disclosure or loss of Confidential Information other than as permitted by this DUA shall be presumed to be a Breach

unless Contractor demonstrates, based on a risk assessment, that there is a low probability that the Confidential Information has been compromised.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to Contractor or that Contractor may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following:

(1) Education records as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g; 34 C.F.R. Part 99

(2) Federal Tax Information as defined in Internal Revenue Code §6103 and Internal Revenue Service Publication 1075;

(3) Personal Identifying Information (PII) as defined in Texas Business and Commerce Code, Chapter 521;

(4) Protected Health Information (PHI) in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information as defined in 45 C.F.R. §160.103;

(5) Sensitive Personal Information (SPI) as defined in Texas Business and Commerce Code, Chapter 521;

(6) Social Security Administration Data, including, without limitation, Medicaid information means disclosures of information made by the Social Security Administration or the Centers for Medicare and Medicaid Services from a federal system of records for administration of federally funded benefit programs under the Social Security Act, 42 U.S.C., Chapter 7;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Destroy", "Destruction", for Confidential Information, means:

(1) Paper, film, or other hard copy media have been shredded or destroyed such that the Confidential Information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(2) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization," such that the Confidential Information cannot be retrieved.

"Discover, Discovery" means the first day on which a Breach becomes known to Contractor, or, by exercising reasonable diligence would have been known to Contractor.

"Legally Authorized Representative" of an individual, including as provided in 45 CFR 435.923 (authorized representative); 45 CFR 164.502(g)(1) (personal representative); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164 (medical power of attorney); and Texas Estates Code § 22.031 (representative).

"Required by Law" means a mandate contained in law that compels an entity to use or disclose Confidential Information that is enforceable in a court of law, including court orders, warrants, subpoenas or investigative demands.

"Subcontractor" means a person who contracts with a prime contractor to work, to supply commodities, or to contribute toward completing work for a governmental entity.

"Workforce" means employees, volunteers, trainees or other persons whose performance of work is under the direct control of a party, whether or not they are paid by that party.

ARTICLE 3. CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

Section 3.01 Obligations of Contractor

Contractor agrees that:

(A) With respect to PHI, Contractor shall:

(1) Make PHI available in a designated record set if requested by HHS, if Contractor maintains PHI in a designated record set, as defined in HIPAA.

(2) Provide to HHS data aggregation services related to the healthcare operations Contractor performs for HHS pursuant to the Base Contract, if requested by HHS, if Contractor provides data aggregation services as defined in HIPAA.

(3) Provide access to PHI to an individual who is requesting his or her own PHI, or such individual's Legally Authorized Representative, in compliance with the requirements of HIPAA.

(4) Make PHI available to HHS for amendment, and incorporate any amendments to PHI that HHS directs, in compliance with HIPAA.

(5) Document and make available to HHS, an accounting of disclosures in compliance with the requirements of HIPAA.

(6) If Contractor receives a request for access, amendment or accounting of PHI by any individual, promptly forward the request to HHS or, if forwarding the request would violate HIPAA, promptly notify HHS of the request and of Contractor's response. HHS will respond to all such requests, unless Contractor is Required by Law to respond or HHS has given prior written consent for Contractor to respond to and account for all such requests.

(B) With respect to ALL Confidential Information, Contractor shall:

(1) Exercise reasonable care and no less than the same degree of care Contractor uses to protect its own confidential, proprietary and trade secret information to prevent Confidential Information from being used in a manner that is not expressly an Authorized Purpose or as Required by Law. Contractor will access, create, maintain, receive, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses.

(2) Establish, implement and maintain appropriate procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, in accordance with applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as Contractor has such Confidential Information in its actual or constructive possession.

(3) Implement, update as necessary, and document privacy, security and Breach notice policies and procedures and an incident response plan to address a Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Base Contract. Contractor shall

produce, within three business days of a request by HHS, copies of its policies and procedures and records relating to the use or disclosure of Confidential Information.

(4) Obtain HHS's prior written consent to disclose or allow access to any portion of the Confidential Information to any person, other than Authorized Users, Workforce or Subcontractors of Contractor who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Breach to Contractor's management and as permitted in Section 3.01(A)(3), above. Contractor shall produce evidence of completed training to HHS upon request. HHS, at its election, may assist Contractor in training and education on specific or unique HHS processes, systems and/or requirements. All of Contractor's Authorized Users, Workforce and Subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code Section 2054.519 by the Texas Department of Information Resources.

(5) Establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Base Contract or applicable law. Contractor shall maintain evidence of sanctions and produce it to HHS upon request.

(6) Obtain prior written approval of HHS, to disclose or provide access to any Confidential Information on the basis that such act is Required by Law, so that HHS may have the opportunity to object to the disclosure or access and seek appropriate relief. If HHS objects to such disclosure or access, Contractor shall refrain from disclosing or providing access to the Confidential Information until HHS has exhausted all alternatives for relief.

(7) Certify that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose and that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. Contractor and its Subcontractors shall maintain at all times an updated, complete, accurate list of Authorized Users and supply it to HHS upon request.

(8) Provide, and shall cause its Subcontractors and agents to provide, to HHS periodic written confirmation of compliance with controls and the terms and conditions of this DUA.

(9) Return to HHS or Destroy, at HHS's election and at Contractor's expense, all Confidential Information received from HHS or created or maintained by Contractor or any of Contractor's agents or Subcontractors on HHS's behalf upon the termination or expiration of this DUA, if reasonably feasible and permitted by law. Contractor shall certify in writing to HHS that all such Confidential Information has been Destroyed or returned to HHS, and that Contractor and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, Contractor acknowledges and agrees that it may not Destroy any Confidential Information if federal or state law, or HHS record retention policy or a litigation hold notice prohibits such Destruction. If such return or Destruction is not reasonably feasible, or is impermissible by law, Contractor shall immediately notify HHS of the reasons such return or Destruction is not feasible and agree to extend the protections of this DUA to the Confidential Information for as long as Contractor maintains such Confidential Information.

(10) Complete and return with the Base Contract to HHS, attached as Attachment 2 to this DUA, the HHS Security and Privacy Initial Inquiry (SPI) at https://hhs.texas.gov/laws-regulations/forms/miscellaneous/hhs-information-security-privacy-initial-inquiry-spi**.** The SPI identifies basic privacy and security controls with which Contractor must comply to protect Confidential Information. Contractor shall comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law, based on the type of Confidential Information Contractor creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. Contractor's

security controls shall be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. Contractor shall update its security controls assessment whenever there are significant changes in security controls for HHS Confidential Information and shall provide the updated document to HHS. HHS also reserves the right to request updates as needed to satisfy state and federal monitoring requirements.

(11) Comply with the HHS Acceptable Use Policy (AUP) and require each Subcontractor and Workforce member who has direct access to HHS Information Resources, as defined in the AUP, to execute an HHS Acceptable Use Agreement.

(12) Only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. A secure transmission of electronic Confidential Information *in motion* includes secure File Transfer Protocol (SFTP) or encryption at an appropriate level as required by rule, regulation or law. Confidential Information *at rest* requires encryption unless there is adequate administrative, technical, and physical security as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information shall be through secure systems. Contractor shall provide proof of system, media or device security and/or encryption to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit, or the Discovery of a Breach. HHS may also request production of proof of security at other times as necessary to satisfy state and federal monitoring requirements. Deidentification of Confidential Information in accordance with HIPAA de-identification standards is deemed secure.

(13) Designate and identify a person or persons, as Privacy Official and Information Security Official, each of whom is authorized to act on behalf of Contractor and is responsible for the development and implementation of the privacy and security requirements in this DUA. Contractor shall provide name and current address, phone number and e-mail address for such designated officials to HHS upon execution of this DUA and prior to any change. Upon written notice from HHS, Contractor shall promptly remove and replace such official(s) if such official(s) is not performing the required functions.

(14) Make available to HHS any information HHS requires to fulfill HHS's obligations to provide access to, or copies of, Confidential Information in accordance with applicable laws, regulations or demands of a regulatory authority relating to Confidential Information. Contractor shall provide such information in a time and manner reasonably agreed upon or as designated by the applicable law or regulatory authority.

(15) Comply with the following laws and standards ***if applicable to the type of Confidential Information and Contractor's Authorized Purpose***:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;
- OMB Memorandum 17-12;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;

- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI;
- Family Educational Rights and Privacy Act
- Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that Contractor supports on behalf of HHS.

(16) Be permitted to use or disclose Confidential Information for the proper management and administration of Contractor or to carry out Contractor's legal responsibilities, except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, if:

(a) Disclosure is Required by Law;

(b) Contractor obtains reasonable assurances from the person to whom the information is disclosed that the person shall:

1. Maintain the confidentiality of the Confidential Information in accordance with this DUA;

2. Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the person; and

3. Notify Contractor in accordance with Section 4.01 of a Breach of Confidential Information that the person Discovers or should have Discovered with the exercise of reasonable diligence.

(C) With respect to ALL Confidential Information, Contractor shall NOT:

(1) Attempt to re-identify or further identify Confidential Information that has been deidentified, or attempt to contact any persons whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS.

(2) Engage in prohibited marketing or sale of Confidential Information.

(3) Permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of HHS without requiring that Subcontractor first execute either the Form Subcontractor Agreement, Attachment 1, or Contractor's own Subcontractor agreement that ensures that the Subcontractor shall comply with the same safeguards and restrictions contained in this DUA for Confidential Information. Contractor is directly responsible for its Subcontractors' compliance with, and enforcement of, this DUA.

ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

Section 4.01. Cooperation and Financial Responsibility.

(A) Contractor shall, at Contractor's expense, cooperate fully with HHS in investigating, mitigating to the extent practicable, and issuing notifications as directed by HHS, for any Breach of Confidential Information.

(B) Contractor shall make Confidential Information in Contractor's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach.

(C) Contractor's obligation begins at the Discovery of a Breach and continues as long as related activity continues, until all effects of the Breach are mitigated to HHS's satisfaction (the "incident response period").

Section 4.02. Initial Breach Notice.

For federal information ***obtained from a federal system of records***, including Federal Tax Information and Social Security Administration Data (which includes Medicaid and other governmental benefit program Confidential Information), Contractor shall notify HHS of the Breach within the first consecutive clock hour of Discovery. The Base Contract shall specify whether Confidential Information is obtained from a federal system of records. For all other types of Confidential Information Contractor shall notify HHS of the Breach not more than 24 hours after Discovery, ***or in a timeframe otherwise approved by HHS in writing.*** Contractor shall initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us and to the HHS division responsible for the Base Contract.

Contractor shall report all information reasonably available to Contractor about the Breach.

Contractor shall provide contact information to HHS for Contractor's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

Section 4.03 Third Business Day Notice: No later than 5 p.m. on the third business day after Discovery, or a time within which Discovery reasonably should have been made by Contractor of a Breach of Confidential Information, Contractor shall provide written notification to HHS of all reasonably available information about the Breach, and Contractor's investigation, including, to the extent known to Contractor***:***
a. The date the Breach occurred;

b. The date of Contractor's and, if applicable, Subcontractor's Discovery;

c. A brief description of the Breach, including how it occurred and who is responsible (or hypotheses, if not yet determined);

d. A brief description of Contractor's investigation and the status of the investigation;

e. A description of the types and amount of Confidential Information involved;

f. Identification of and number of all individuals reasonably believed to be affected, including first and last name of the individual and if applicable, the Legally authorized representative, last known address, age, telephone number, and email address if it is a preferred contact method;

g. Contractor's initial risk assessment of the Breach demonstrating whether individual or other notices are required by applicable law or this DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

h. Contractor's recommendation for HHS's approval as to the steps individuals and/or Contractor on behalf of individuals, should take to protect the individuals from potential harm, including Contractor's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;

i. The steps Contractor has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

j. The steps Contractor has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Breach;

k. Identify, describe or estimate of the persons, Workforce, Subcontractor, or individuals and any law enforcement that may be involved in the Breach;

l. A reasonable schedule for Contractor to provide regular updates regarding response to the Breach, but no less than every three (3) business days, or as otherwise directed by HHS in writing, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

m. Any reasonably available, pertinent information, documents or reports related to a Breach that HHS requests following Discovery.

Section 4.04. Investigation, Response and Mitigation.

(A) Contractor shall immediately conduct a full and complete investigation, respond to the Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to HHS for incident response purposes and for purposes of HHS's compliance with report and notification requirements, to the satisfaction of HHS.

(B) Contractor shall complete or participate in a risk assessment as directed by HHS following a Breach, and provide the final assessment, corrective actions and mitigations to HHS for review and approval.

(C) Contractor shall fully cooperate with HHS to respond to inquiries and/or proceedings by state and federal authorities, persons and/or individuals about the Breach.

(D) Contractor shall fully cooperate with HHS's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHS in a Corrective Action Plan if directed by HHS under the Base Contract.

Section 4.05. Breach Notification to Individuals and Reporting to Authorities.

(A) HHS may direct Contractor to provide Breach notification to individuals, regulators or third-parties, as specified by HHS following a Breach.

(B) Contractor must comply with all applicable legal and regulatory requirements in the time, manner and content of any notification to individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in Contractor's name and on Contractor's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of Contractor's representative, an email address and a toll-free telephone number, for the individual to obtain additional information.

(C) Contractor shall provide HHS with draft notifications for HHS approval prior to distribution and copies of distributed and approved communications.

(D) Contractor shall have the burden of demonstrating to the satisfaction of HHS that any required notification was timely made. If there are delays outside of Contractor's control, Contractor shall provide written documentation to HHS of the reasons for the delay.

(E) If HHS directs Contractor to provide notifications, HHS shall, in the time and manner reasonably requested by Contractor, cooperate and assist with Contractor's information requests in order to make such notifications.

ARTICLE 5. GENERAL PROVISIONS

Section 5.01 Ownership of Confidential Information

Contractor acknowledges and agrees that the Confidential Information is and shall remain the property of HHS. Contractor agrees it acquires no title or rights to the Confidential Information.

Section 5.02 HHS Commitment and Obligations

HHS will not request Contractor to create, maintain, transmit, use or disclose PHI in any manner that would not be permissible under applicable law if done by HHS.

Section 5.03 HHS Right to Inspection

At any time upon reasonable notice to Contractor, or if HHS determines that Contractor has violated this DUA, HHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of Contractor to monitor compliance with this DUA. For purposes of this subsection, HHS's agent(s) include, without limitation, the HHS Office of the Inspector General, the Office of the Attorney General of Texas, the State Auditor's Office, outside consultants, legal counsel or other designee.

Section 5.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which Contractor executes the Base Contract and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended, this DUA is extended to run concurrent with the Base Contract.

(A) If HHS determines that Contractor has violated a material term of this DUA; HHS may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA and/or the Base Contract; or

(2) Require Contractor to submit to a corrective action plan, including a plan for monitoring and plan for reporting as HHS may determine necessary to maintain compliance with this DUA; or

(3) Provide Contractor with a reasonable period to cure the violation as determined by HHS; or

(4) Terminate the DUA and Base Contract immediately and seek relief in a court of competent jurisdiction in Travis County, Texas.

Before exercising any of these options, HHS will provide written notice to Contractor describing the violation and the action it intends to take.

(B) If neither termination nor cure is feasible, HHS shall report the violation to the applicable regulatory authorities.

(C) The duties of Contractor or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to HHS, as required by this DUA.

Section 5.05 Injunctive Relief

(A) Contractor acknowledges and agrees that HHS may suffer irreparable injury if Contractor or its Subcontractor fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) Contractor further agrees that monetary damages may be inadequate to compensate HHS for Contractor's or its Subcontractor's failure to comply. Accordingly, Contractor agrees that HHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

Section 5.06 Indemnification

Contractor shall indemnify, defend and hold harmless HHS and its respective Executive Commissioner, employees, Subcontractors, agents (including other state agencies acting on behalf of HHS) or other members of HHS' Workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this DUA or from any acts or omissions related to this DUA by Contractor or its employees, directors, officers, Subcontractors, or agents or other members of Contractor's Workforce. The duty to indemnify, defend and hold harmless is independent of the duty to insure. Upon demand, Contractor shall reimburse HHS for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including costs of required notices, investigation, and mitigation of a Breach, fines or penalties imposed on an Indemnified Party by a regulatory authority, and reasonable attorneys' fees) which may be imposed upon any Indemnified Party to the extent caused by and which results from the Contractor's failure to meet any of its obligations under this DUA. Contractor's obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this DUA.

Section 5.07 Insurance

(A) In addition to any insurance required in the Base Contract, at HHS's option, HHS may require Contractor to maintain, at its expense, the special and/or custom first- and third-party insurance coverages, including without limitation data breach, cyber liability, crime theft and notification expense coverages, with policy limits sufficient to cover any liability arising under this DUA, naming the State of Texas, acting through HHS, as an additional named insured and loss payee, with primary and noncontributory status.

(B) Contractor shall provide HHS with written proof that required insurance coverage is in effect, at the request of HHS.

Section 5.08 Entirety of the Contract

This DUA is incorporated by reference into the Base Contract and, together with the Base Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced.

Section 5.09 Automatic Amendment and Interpretation

Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on HHS

and/or Contractor remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits HHS and Contractor to comply with laws applicable to Confidential Information.

Section 5.10 Notices; Requests for Approval

All notices and requests for approval related to this DUA must be directed to the HHS Chief Privacy Officer at privacy@hhsc.state.tx.us.

ATTACHMENT 1. SUBCONTRACTOR AGREEMENT FORM

HHS CONTRACT NUMBER

_____

The DUA between HHS and Contractor establishes the permitted and required uses and disclosures of Confidential Information by Contractor.

Contractor has subcontracted with_____ (Subcontractor) for performance of duties on behalf of CONTRACTOR which are subject to the DUA. Subcontractor acknowledges, understands and agrees to be bound by the same terms and conditions applicable to Contractor under the DUA, incorporated by reference in this Agreement, with respect to HHS Confidential Information. Contractor and Subcontractor agree that HHS is a third-party beneficiary to applicable provisions of the subcontract.

HHS has the right, but not the obligation, to review or approve the terms and conditions of the subcontract by virtue of this Subcontractor Agreement Form.

Contractor and Subcontractor assure HHS that any Breach as defined by the DUA that Subcontractor Discovers shall be reported to HHS by Contractor in the time, manner and content required by the DUA.

If Contractor knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by Subcontractor that constitutes a material breach or violation of the DUA or the Subcontractor's obligations, Contractor shall:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract or arrangement with Subcontractor, if feasible;
3. Notify HHS immediately upon Discovery of the pattern of activity or practice of Subcontractor that constitutes a material breach or violation of the DUA and keep HHS reasonably and regularly informed about steps Contractor is taking to cure or end the violation or terminate Subcontractor's contract or arrangement.

This Subcontractor Agreement Form is executed by the parties in their capacities indicated below.

CONTRACTOR	**SUBCONTRACTOR**
BY: _____	**BY:** _____
NAME: _____	**NAME:**_____
TITLE: _____	**TITLE:**_____
DATE _____, _____	**DATE:**_____

Attachment 2-
Security and Privacy Initial Inquiry
[Attach Completed SPI Here]

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

Between	Entity listed on the Order Form selling the Cloud Service **("Qualtrics")**
And	Entity listed on the Order Form purchasing the Cloud Service **("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 and non-transferable right to use the Cloud Service (including its implementation and configuration), Cloud Materials and Documentation solely for Customer's and its Affiliates' internal business operations. Customer may use the Cloud Service world-wide except from countries or regions where such use is prohibited by Export Laws or as set forth in an Order Form. 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) copy, translate, disassemble, decompile, make derivative works, or reverse engineer the Cloud Service (or attempt any of the foregoing),

(b) enter, store, or transfer any content or data on or via the Cloud Service that is unlawful or infringes any intellectual property rights,

(c) circumvent or endanger its operation or security, or

(d) remove Qualtrics' copyright and authorship notices.

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.

Via the Cloud Service, Customer may access integrations with web services made available by third parties 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.

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 or the Documentation.

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**") in compliance with applicable data protection law.

3.4 Modifications.

(a) Subject to Section 3.4(b) below, the Cloud Service may be modified by Qualtrics. Qualtrics will inform Customer of modifications by email (if the modification is not solely an enhancement), the support portal, release notes, Documentation or the Cloud Service. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.

(b) If a modification materially degrades the overall functionality of the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to Qualtrics within 30 days after receipt of Qualtrics' informational notice and receive a refund as set forth in Section 6.3.

3.5 Analyses.

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

(b) Personal data contained in Customer Data is only used to provide the Cloud Service and Professional Services to Customer and its Authorized Users.

(c) Analyses may be used for the following purposes:

(1) product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new Qualtrics products and services,
(2) improving resource allocation and support,
(3) internal demand planning,
(4) training and developing machine learning algorithms,
(5) improving product performance,
(6) verification of security and data integrity
(7) 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 and use Customer Data to provide and support the Cloud Service and as set out in the Agreement.

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.

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 to perform a final export of Customer Data from the Cloud Service. Alternatively, if self-service export tools are unavailable, Customer may request data export through support ticket.

(c) After 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. If Customer does not pay fees in accordance with the terms of the Agreement, then, after prior written notice, Qualtrics may suspend Customer's use of the applicable Cloud Service until payment is made. Any fees not paid when due shall accrue interest at the maximum legal rate. Purchase orders are for administrative convenience only. Qualtrics may issue an invoice and collect payment without a corresponding purchase order. Customer will not withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable. All fees are non-refundable except as set forth in Sections 6.3 and 7.4.

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. 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, Customer will reimburse Qualtrics for those amounts 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 party may terminate the Agreement:

(a) upon 30 days' prior written notice of the other party's material breach of the Agreement unless the breach is cured during that 30-day period,

(b) as permitted under Sections 3.4(b), 7.3(b), 7.4(c), 8.1(c), or 12.4 (with termination effective 30 days after receipt of notice in each of these cases), or

(c) immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

6.3 Refund and Payments.

For termination by Customer or an 8.1(c) or 12.4 termination, Customer will be entitled to:

(a) a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective date of termination (unless such refund is prohibited by Export Laws), and

(b) a release from the obligation to pay fees due for periods after the effective date of termination.

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 retained, returned, or destroyed as required by the Agreement or applicable law, 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.

Customer's sole and exclusive remedies and Qualtrics' entire liability for breach of the warranty under Section 7.2 will be:

(a) the correction of the deficient Cloud Service, and

(b) if Qualtrics fails to correct the deficient Cloud Service, Customer may terminate its subscription for the affected Cloud Service and receive a refund as set forth in Section 6.3. Any termination must occur within three months after Qualtrics' failure to correct the deficient Cloud Service.

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 30 days after the failure and receive a refund as set forth in Section 6.3.

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 and indemnify (as set forth in the next sentence) Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's or 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) use of the Cloud Service not permitted under the Agreement, (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) If a third party makes a claim or in Qualtrics' reasonable opinion is likely to make such a claim, Qualtrics may at its sole option and expense (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 and Customer may receive a refund as set forth in Section 6.3.

8.2 Claims Brought Against Qualtrics.

Customer will defend and indemnify , to the extent allowed under the laws of the state of Texas, Qualtrics against claims brought against Qualtrics and its Affiliates and subcontractors by any third party related to Customer Data.

8.3 Third Party Claim Procedure.

All third party claims under Section 8 shall be conducted as follows:

(a) The party against whom a third party claim is brought (the "**Indemnified Party**") will timely notify the other party (the "**Indemnifying Party**") in writing of any claim. The Indemnified Party will reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the Indemnifying Party subject to Section 8.3(b).

(b) The Indemnifying Party 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 Indemnified Party.

(d) The Indemnifying Party's obligations will not apply if the Indemnified Party's failure to timely notify the Indemnifying Party in writing of any such claim prejudices the Indemnifying Party.

8.4 Exclusive Remedy.

The provisions of Section 8 state the sole, exclusive, and entire liability of the parties and their Affiliates, Business Partners and subcontractors to the other party, and is the other party's sole remedy, with respect to covered third party claims and to the infringement or misappropriation of third party intellectual property rights.

9. LIMITATION OF LIABILITY

9.1 Unlimited Liability.

Neither party's liability is capped for damages resulting from:

(a) the parties' obligations under Section 8.1(a) and 8.2,

(b) death or bodily injury arising from either party's gross negligence or willful misconduct, or

(c) Customer's unauthorized use of any Cloud Service or any failure by Customer to pay any fees due under the Agreement.

9.2 Liability Cap.

Except as set forth in Section 9.1, the maximum aggregate liability of either party (or its respective Affiliates or Qualtrics' subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any 12-month period will not exceed the annual fees paid for the applicable Cloud Service or Professional Service associated with the damages for that 12-month period. Any "12-month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3 Exclusion of Damages.

In no case will:

(a) either party (or its respective Affiliates or Qualtrics' subcontractors) be liable to the other party for any special, incidental, consequential, or indirect damages, loss of goodwill or business profits, work stoppage or for exemplary or punitive damages; or

(b) Qualtrics be liable for any damages caused by any Cloud Service provided for no fee.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 QUALTRICS Ownership.

Except for any rights expressly granted to Customer under the Agreement, Qualtrics, Qualtrics' Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Professional Services, design contributions, related knowledge or processes, and any derivative works of them.

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.

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

(a) The receiving party shall:

(1) maintain all Confidential Information of the disclosing party in strict confidence, taking steps to protect the disclosing party's Confidential Information substantially similar to those steps that the receiving party takes to protect its own Confidential Information, which shall not be less than a reasonable standard of care;

(2) not disclose any Confidential Information of the disclosing party to any person other than its Representatives 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;

(3) not use or reproduce any Confidential Information of the disclosing party for any purpose outside the scope of the Agreement; and

(4) retain any and all confidential, internal, or proprietary notices or legends that appear on the original and on any reproductions.

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

(c) The receiving party may disclose the disclosing party's Confidential Information to the extent required by law, regulation, court order, or regulatory agency, on the condition that the receiving party required to make such a disclosure uses reasonable efforts to give the disclosing party reasonable prior notice of such required disclosure (to the extent legally permitted) and provides reasonable assistance in contesting the required disclosure, at the request and cost of the disclosing party. The receiving party and its Representatives shall use commercially reasonable efforts to disclose only that portion of the Confidential Information that is legally requested to be disclosed and shall request that all Confidential Information that is so disclosed is accorded confidential treatment.

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) has become generally known or available to the public through no act or omission by the receiving party,

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

(d) is lawfully acquired free of restriction by the receiving party from a third party having the right to furnishsuch Confidential Information, or

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

11.3 Destruction of Confidential Information.

Upon the disclosing party's request, the receiving party shall promptly destroy or return the disclosing party's Confidential Information, including copies and reproductions thereof. The obligation to destroy or return Confidential Information will not apply:

(a) if legal proceedings related to the Confidential Information prohibit its return or destruction, until the proceedings are settled or a final judgment is rendered;

(b) to Confidential Information held in archive or back-up systems under general systems archiving or backup policies; or

(c) to Confidential Information the receiving party is legally required to retain.

12. MISCELLANEOUS

12.1 Severability.

If any provision of the Agreement is held to be wholly or in part 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 Counterparts.

The Agreement may be signed in counterparts, each of which is an original and together constitute one Agreement. Electronic signatures that comply with applicable law are deemed original signatures.

12.4 Trade Compliance.

(a) Qualtrics and Customer shall comply with Export Laws in the performance of this Agreement. Qualtrics' Confidential Information is subject to Export Laws. Customer 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 Cuba, Iran, the People's Republic of Korea (North Korea), Syria, Donetsk People's Republic (DNR), Luhansk People's Republic (LNR), or Crimea/Sevastopol regions.

(b) Upon Qualtrics' request, Customer shall provide information and documents to support obtaining an export authorization. Upon written notice to Customer, Qualtrics may immediately terminate Customer's subscription to the affected Cloud Service if:

(1) the competent authority does not grant such export authorization within 18 months; or

(2) Export Laws prohibit Qualtrics from providing the Cloud Service or Professional Services to Customer.

12.5 Notices.

All notices will be in writing and given when delivered to, (a) in the case of Qualtrics, notice@qualtrics.com with a physical copy to Qualtrics, Attn: Legal, 333 W River Park Dr, Provo UT 84604, USA, or, (b) in the case of Customer, the email or physical address set forth in an Order Form or Agreement. Notices from Qualtrics to Customer may be in the form of an electronic notice to Customer's authorized representative or administrator. Qualtrics may provide system notifications and information relating to the operation, hosting, or support of the Cloud Service within the Cloud Service or make such notifications available via the Qualtrics support portal. Customer shall maintain up-to-date notice contact information within the Cloud Service.

12.6 Assignment.

Without Qualtrics' prior written consent, Customer may not assign, delegate, 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 Professional 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.

Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 Governing Law.

12.11 The contract shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the contract is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to the contracting Agency. Entire Agreement.

The Agreement, DIR-TSO-4288, and Customer Purchase Order # constitute 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 the Agreement.

12.12 Feedback.

Customer may at its sole discretion provide Qualtrics with Feedback, in which case, Qualtrics Affiliates may retain and freely use such Feedback without restriction, compensation, or attribution to the source of the Feedback.

12.13 Data Processing Agreement.

The DPA will govern the processing of any personal data in the Cloud Service.

Glossary

1.1 **"Affiliate"** means any legal entity in which Customer or Qualtrics' Parent Company, directly or indirectly, holds more than 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, including this GTC.

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 Customer, Customer's Affiliates, or 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 consultants, distributors, service providers, or suppliers of Customer and its Affiliates.

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 Analyses and materials provided or developed in the delivery of any support or Professional Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.

1.7 "**Confidential Information"** means all information that the disclosing party protects against unrestricted disclosure to others that (a) the disclosing party or its representatives designate as confidential, internal, or proprietary at the time of disclosure, or (b) should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.

1.8 **"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 Qualtrics' Confidential Information.

1.9 **"Documentation"** means Qualtrics' then-current technical and functional documentation, including any roles and responsibilities descriptions relating to the Cloud Services that Qualtrics makes available to Customer under the Agreement.

1.10 "**Export Laws**" means all applicable import, export control, and sanctions laws, including thelaws of the United States.

1.11 "**Feedback**" means input, comments, or suggestions regarding Qualtrics' business and technology direction and the possible creation, modification, correction, improvement, or enhancement of the Cloud Service or Cloud Materials.

1.12 **"Order Form"** means the medium by which Customer purchases a Cloud Service, including, as applicable, an ordering document that references the GTC.

1.13 **"Professional Services"** means implementation services, consulting services, or other related services provided under an Order Form.

1.14 **"Qualtrics' Parent Company"** means SAP SE, majority shareholder of Qualtrics.

1.15 **"Representatives"** means a party's Affiliates, employees, contractors, sub-contractors, legal representatives, accountants, or other professional advisors.

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

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

1.18 **"Taxes"** means all transactional taxes, levies, and similar charges (and any related interest and penalties), such as federal, state or local sales tax, value added tax, goods and services tax, use tax, excise tax, service tax, or similar taxes.

1.19 **"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.

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 natural 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. **"EU Standard Contractual Clauses"** means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof as adopted by Qualtrics. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.3.

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

1.7. **"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 EU Standard Contractual Clauses.

1.8. **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:

a) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service; or

b) supplied to or accessed by Qualtrics or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

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 Annex with respect to the EU Standard Contractual Clauses.

1.13. **"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.

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

1.15. **"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, 2 and 3 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), applicable Technical and Organizational Measures (Schedule 2), and the UK addendum to the EU Standard Contractual Clauses, if applicable (Schedule 3).

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 EU Standard Contractual Clauses

Sections 8.3 to 8.6 apply in respect of 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 EU Standard Contractual Clauses as may be amended in accordance with applicable Data Protection Law.

8.3. Applicability of EU Standard Contractual Clauses where Qualtrics is not located in a Third Country

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

8.4. Applicability of EU Standard Contractual Clauses where Qualtrics is located in a Third Country

8.4.1. Where Qualtrics is located in a Third Country, or in a country that otherwise requires use of the EU Standard Contractual Clauses for transfers of Personal Data to that country, Qualtrics and Customer hereby enter into the EU Standard Contractual Clauses with Customer as the data exporter and Qualtrics as the data importer 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 EU Standard Contractual Clauses, Qualtrics acknowledges that Customer acts as Processor under the instructions of its Controller(s).

Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the EU Standard Contractual Clauses with Qualtrics in the same manner as Customer in accordance with Section 8.4.1 above. In such case, Customer enters into the EU Standard Contractual Clauses on behalf of other Controllers or Processors.

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

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 Qualtrics 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.

8.4.3. On request from a Data Subject, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and Qualtrics (including the relevant Schedules) available to Data Subjects.

8.5. Applicability of EU Standard Contractual Clauses where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses

Subject to Sections 8.2 to 8.4, where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses, then the EU Standard Contractual Clauses are interpreted as follows:

8.5.1. In relation to the Swiss Data Protection Act ("**FDPA**"):

a) the references to a "Member State" in the EU Standard Contractual Clauses will be deemed to include Switzerland;

b) references to the law of the European Union or of a Member State in the EU Standard Contractual Clauses shall be deemed to be a reference to the FDPA;

c) the Swiss Federal Data Protection and Information Commissioner will be the sole or, where both the FDPA and the GDPR apply to such transfer, one of the competent data protection authorities, under the EU Standard Contractual Clauses;

d) the terms used in the EU Standard Contractual Clauses that are defined in the FDPA will be construed to have the meaning of the FDPA; and

e) where the FDPA protects legal entities as data subjects, the EU Standard Contractual Clauses will apply to data relating to identified or identifiable legal entities.

8.5.2. In relation to the Data Protection Act 2018 of the United Kingdom ("**UK GDPR**"), from 21 September 2022, the EU Standard Contractual Clauses shall be interpreted and construed in accordance with the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of UK GDPR on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, and attached at Schedule 3 (the "**Approved Addendum**"). Schedules 1 and 2 set out the information for Part 1, Tables of the Approved Addendum.

8.6. Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the EU 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 EU Standard Contractual Clauses.

9. DOCUMENTATION; RECORDS OF PROCESSING

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 EU Standard Contractual Clauses and applicable Data Protection Law.

1. Optional Clauses Of The EU Standard Contractual Clauses

1.1. Except where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses then the governing law of the EU Standard Contractual Clauses shall be the laws of Ireland.

1.2. The optional Clauses 7 and the option in Clause 11a of the EU Standard Contractual Clauses shall not apply.

1.3. Option 2, General Written Authorisation of Clause 9 shall apply in accordance with the notification periods set out in Section 7 of this DPA.

2. LIST OF PARTIES

2.1. Under the EU Standard Contractual Clauses

2.1.1. 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.

2.1.2. 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.

3. DESCRIPTION OF TRANSFER

3.1. 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.

3.2. Data Categories

The transferred Personal Data concerns the following categories of data:
Customer determines the categories of data and/or data fields which could be transferred 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 transferred or entered into the Cloud Service.

3.3. Special Data Categories (if agreed)

3.3.1. 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.

3.3.2. 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.

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

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

3.4.1. 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.

3.4.2. 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.

3.5. Additional description in respect of the EU Standard Contractual Clauses:

3.5.1. The purpose of the transfer is to provide and support the relevant Cloud Service. Qualtrics and its Subprocessors may provide or support the Cloud Service remotely.

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

3.5.3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Personal Data will be transferred on an ongoing basis for the duration of the Agreement.

3.5.4. 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 of the DPA.

4. COMPETENT SUPERVISORY AUTHORITY

4.1. In respect of the EU Standard Contractual Clauses:

4.1.1. Module 2: Transfer Controller to Processor

4.1.2. Module 3: Transfer Processor to Processor

4.2. 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 EU 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 EU 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.

Schedule 3 - International Data Transfer Addendum to the EU Standard Contractual Clauses: Tables

Table 1: Parties

Addendum Effective Date / Start date	Either (a) 21st September 2022, where the effective date of the Agreement is before 21st September 2022; or (b) otherwise, on the effective date of the Agreement. Notwithstanding the Effective Date of this Addendum, Customer acknowledges that Qualtrics will implement the UK Addendum with subprocessors within the time period permitted by applicable law, and at the Effective Date of this Addendum, the UK Addendum may not be in place with subprocessors.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer	Qualtrics
Key Contact	See details in Schedule 1 of the DPA. Customer's Data Protection Officer or other legal representative shall be the key contact. Customer shall make these details available upon Qualtrics' request.	See details in Schedule 1 of the DPA. Qualtrics' Data Protection Officer or other legal representative shall be the key contact. Qualtrics shall make these details available upon Customer's request.

(a) Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs, which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date of the DPA Reference: the EU Standard Contractual Clauses referenced in the DPA

(b) Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Schedule 1 of the DPA
Annex 1B: Description of Transfer: See Schedule 1 of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2 of the DPA

(c) Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party