CITY OF SAN ANTONIO

FINANCE DEPARTMENT, PURCHASING DIVISION

REQUEST FOR COMPETITIVE SEALED PROPOSAL ("RFCSP")
NO.: **6100015294; 2022-079**

RIDESHARE MONITORING SERVICES
FOR SAN ANTONIO INTERNATIONAL AIRPORT

Date Issued: **AUGUST 17, 2022**

PROPOSALS MUST BE RECEIVED **NO LATER** THAN:
2:00 PM, CENTRAL TIME, SEPTEMBER 23, 2022

Proposals may be submitted by the following means:
Electronic submission through the portal

Response submissions will only be accepted electronically

Proposal Due Date: 2:00 p.m., Central Time, SEPTEMBER 23, 2022

RFCSP No.: 6100015294; 2022-079

Respondent's Name and Address

Proposal Bond: No Performance Bond: No Payment Bond: No Other: No

See Supplemental Terms & Conditions for information on these requirements.

Affirmative Procurement Initiative: No DBE / ACDBE Requirements: None

See Instructions for Respondents and Attachments sections for more information on these requirements.

Pre-Proposal Conference * YES

*If YES, the Pre-Proposal conference will be held on **AUGUST 26, 2022, at 2:00 P.M. CT** at **San Antonio International Airport, Terminal A Mezzanine Conference Room, 9800 Airport Blvd, San Antonio TX 78216.** Respondents may also call the toll-free number listed below and enter access code and meeting number to participate the day of the conference.

Dial-In Number: 1-415-655-0001
Access Code: 2453 470 8622

Staff Contact Person: MARISOL AMADOR, PROCUREMENT SPECIALIST III, P.O. Box 839966, San Antonio, TX 78283-3966.
Email: MARISOL.AMADOR@SANANTONIO.GOV

SBEDA Contact Information: BARBARA PATTON, 210-207-3592, BARBARA.PATTON@SANANTONIO.GOV

RESTRICTIONS ON COMMUNICATIONS

In accordance with Section 2-61 of the City Code, the following restrictions on communications apply to this solicitation: Respondents are prohibited from contacting 1) City officials, as defined by §2-62 of the City Code of the City of San Antonio, regarding the RFCSP or proposal from the time the RFCSP has been released until the contract is posted for consideration as an agenda item during a meeting designated as an "A" session; and 2) City employees from the time the RFCSP has been released until the contract is approved at a City Council "A" session.

Restrictions extend to "thank you" letters, phone calls, emails and any contact that results in the direct or indirect discussion of the RFCSP and/or proposal submitted by Respondent.

Violation of this provision by Respondent and/or its agent may lead to disqualification of Respondent's proposal from consideration.

For additional information, see the section of this RFCSP entitled "Restrictions on Communication".

002 - TABLE OF CONTENTS

003 - INSTRUCTIONS FOR RESPONDENTS

PART A

Submission of Proposals. Respondents must submit proposals electronically.

Submission of Electronic Proposals. Submit one **COMPLETE** proposal electronically by the due date provided on the Cover Page. All times stated herein are Central Time. Any proposal or modification received after the time and date stated on the Cover Page shall be rejected.

Proposals sent to City by facsimile or email shall be rejected.

Modified Proposals. Proposals may be modified provided such modifications are received prior to the time and date set for submission of proposals. A modified proposal will automatically replace a prior proposal submission. See below for information on submitting Alternate Proposals.

City shall not be responsible for lost or misdirected proposals or modifications.

Forms Requiring Signatures.

Signature Page. Respondent's electronic submission constitutes a binding signature for all purposes.

All Other Documents. All other forms in this solicitation which require a signature must have a signature affixed thereto by manually signing the document prior to scanning it and uploading it with your submission.

Respondents are cautioned that they are responsible for the security of their log-on ID and password, since unauthorized use could result in Respondent's being held liable for the submission.

Vendor Registration. Respondent is required to register as a vendor with the City prior to the due date for submission of proposals. Respondent may register at the following site: http://www.sanantonio.gov/purchasing/saeps. Respondents must identify the correct name of the entity that will be providing the goods and/or services under the contract. No nicknames, abbreviations (unless part of the legal title), shortened or short-hand names will be accepted in place of the full, true and correct legal name of the entity.

Alternate Proposals. Alternate proposals may be allowed at the sole discretion of City.

Electronic Alternate Proposals Submitted Through the Portal. All alternate proposals submitted electronically are recorded with original proposals when submitted electronically.

Catalog Pricing. (This section applies to proposals using catalog pricing.)

The proposal will be based on manufacturer's latest dated price list(s). Said price list(s) must denote the manufacturer, latest effective date and price.

Respondents shall be responsible for providing one copy of the manufacturer's catalog for each manufacturer for which a proposal is submitted. Respondent shall provide said catalog at the time of submission of its proposal. Manufacturers' catalogs may be submitted in in any of the following formats: paper copy, flash drive, or CD ROM. Catalogs shall be mailed to the Finance Department, Purchasing Division, P.O. Box 839966, San Antonio, Texas 78283-3966 prior to bid opening. Bidder shall submit a PDF file for proposals submitted electronically.

Respondents may submit price lists other than the manufacturer's price list. Said price list(s) must denote the company name, effective date. These price lists are subject to approval of City's Finance Department.

Specified items identified herein, if any, are for overall proposal evaluation and represent the commonly and most used items. Net prices entered for those specified items must reflect the actual price derived from quoted price list less all discounts offered.

Restrictions on Communication.

In accordance with and as authorized by Section 2-61 of the City Code, the following restrictions on communications apply to this solicitation: Respondents are prohibited from contacting 1) City officials, as defined by §2-62 of the City

Code of the City of San Antonio, regarding the RFCSP or proposal from the time the RFCSP has been released until the contract is posted for consideration as an agenda item during a meeting designated as an "A" session; and 2) City employees from the time the RFCSP has been released until the contract is approved at a City Council "A" session.

Restrictions extend to "thank you" letters, phone calls, emails and any contact that results in the direct or indirect discussion of the RFCSP and/or proposal submitted by Respondent.

Violation of this provision by Respondent and/or its agent may lead to disqualification of Respondent's proposal from consideration.

Exceptions to the restrictions on communication with City employees include:

Respondents may ask verbal questions concerning this RFCSP at the Pre-Submittal Conference.

Respondents may submit written questions, or objections to specifications, concerning this RFCSP to the Staff Contact Person listed on the Cover Page on or before 10 calendar days prior to the date proposals are due. Questions received after the stated deadline will not be answered. Questions submitted and City's responses will be posted with this solicitation. All questions shall be sent by e-mail.

Respondents may provide responses to questions asked of them by the Staff Contact Person after proposals are received and opened. The Staff Contact Person may request clarification to assist in evaluating Respondent's response. The information provided is not intended to change the proposal response in any fashion. Such additional information must be provided within two business days from City's request. Respondents may also respond to requests by the Staff Contact Person for best and final offers, which do allow respondents to change their proposals. Requests for best and final offers will be clearly designated as such. During interviews, if any, verbal questions and explanations will be permitted. If interviews are conducted, respondents shall not bring lobbyists. The City reserves the right to exclude any persons from interviews as it deems in its best interests.

Respondents and/or their agents are encouraged to contact the Aviation Department Business Opportunity and Diversity Development for assistance or clarification with issues specifically related to the City's Small Business Economic Development Advocacy (SBEDA) Program policy and/or completion of the required SBEDA forms. The point of contact may be reached by telephone at (210) 207-3592 or by e-mail at BODD@sanantonio.gov. *This exception to the restriction on communication does not apply, and there is no contact permitted to the Small Business Office regarding this solicitation, after the solicitation closing date.*

If this solicitation contains DBE/ACDBE requirements, respondents and/or their agents may contact the Aviation Department's DBE/ACDBE Liaison Officer for assistance or clarification with issues specifically related to the DBE/ACDBE policy and/or completion of the required form(s). The point of contact is Barbara Patton, who may be reached via telephone at (210) 207-3592 or through e-mail at Barbara.Patton@sanantonio.gov. Respondents and/or their agents may contact Ms. Patton at any time prior to the due date for submission of proposals. Contacting her or her office regarding this RFCSP after the proposal due date is not permitted. If this solicitation contains DBE/ACDBE requirements, it will be noted on the Cover Page.

Respondents may contact the Vendor Support staff at (210) 207-0118 or by email at vendors@sanantonio.gov for assistance with vendor registration and submitting electronic proposals.

Upon completion of the evaluation process, Respondents shall receive a notification letter indicating the recommended firm, anticipated City Council agenda date, and a review of the solicitation process.

Pre-Submittal Conference.

If a Pre-Submittal Conference is scheduled, it will be held at the time and place noted on the Cover Page. Respondents are encouraged to prepare and submit their questions in writing in advance of the Pre-Submittal Conference in order to expedite the proceedings. Pre-Submittal Conference participation is optional, but highly encouraged.

Call the Staff Contact Person for information to request an interpreter for the deaf. Interpreters for the deaf must be requested at least 48 hours prior to the meeting. For other assistance, call (210) 207-7245 Voice/TTY.

Any oral response given at the Pre-Submittal Conference that is not confirmed in writing and posted with this solicitation shall not be official or binding on the City.

Changes to RFCSP.

Changes to this RFCSP made prior to the due date for proposals shall be made directly to the original RFCSP. Changes are captured by creating a replacement version each time the RFCSP is changed. It is Respondent's responsibility to check for new versions until the proposal due date. City will assume that all proposals received are based on the final version of the RFCSP as it exists on the day proposals are due.

No oral statement of any person shall modify or otherwise change or affect the terms, conditions or specifications stated in the RFCSP.

Preparation of Proposals.

All information required by the RFCSP must be furnished or the proposal may be deemed non-responsive and rejected. Any ambiguity in the proposal as a result of omission, error, unintelligible or illegible wording shall be construed in the favor of City.

Proposal Format. Websites or URLs shall not be submitted in lieu of the electronic submission through City's portal. **ELECTRONIC** proposals must include **ALL** the sections and attachments in the sequence listed in the RFCSP Section 003, Part B, Submission Requirements, and each section and attachment must be indexed in a Table of Contents page. For electronic submissions, each separate section should be attached as a separate file. Failure to meet the above conditions may result in disqualification of the proposal or may negatively affect scoring.

Correct Legal Name. If Respondent is found to have incorrectly or incompletely stated the name of the entity that will provide goods and/or services, the proposal may be rejected.

Line Item Proposals. Any proposal that is considered for award by each unit or line item must include a price for each unit or line item for which Respondent wishes to be considered. Scoring of pricing for proposals is on the basis of low line item, low total line items, or in any other combination that serves the best interest of City, unless City designates this solicitation as an "all or none" proposal in the Supplemental Terms & Conditions.

All or None Bid. Any proposal that is considered for award on an "all or none" basis must include a price for all units or line items. In an "All or None" bid, a unit price left blank shall result in the proposal being deemed nonresponsive and disqualified from consideration. An "All or None" bid is one in which City will award the entire contract to one respondent only. City reserves the right to delete line items prior to award.

Delivery Dates. Proposed delivery dates must be shown in the proposal where required and shall include weekends and holidays, unless specified otherwise in this RFCSP. Proposed delivery times must be specific. Phrases such as "as required", "as soon as possible" or "prompt" may result in disqualification of the proposal. Special delivery instructions, if any, may be found in the Specifications / Scope of Services section of this document, or in the Purchase Order.

Tax Exemption. The City of San Antonio is exempt from payment of federal taxes, and State of Texas limited sales excise and use taxes. Respondents must not include such taxes in proposal prices. An exemption certificate will be signed by City where applicable upon request by Respondent after contract award.

Description of Supplies.

Any brand names, catalog or manufacturer's reference used in describing an item is merely descriptive, and not restrictive, unless otherwise noted, and is used only to indicate quality and capability desired.

Proposals submitted for comparable items must clearly identify the proposed product, model, and type, as applicable, and shall include manufacturer specification sheet(s) for each proposed item with proposal response. Product specifications shall be the most current available and be sufficiently detailed and descriptive so as to permit City to determine the item's suitability and compliance with proposal specifications. City shall be the sole judge of equality and suitability of comparable items.

Pro-rata adjustments to packaging and pricing may be allowed at the sole discretion of City.

Samples, Demonstrations and Pre-award Testing. If requested by City, Respondent shall provide product samples, demonstrations, and/or testing of items proposed to ensure compliance with specifications prior to award of the contract. Samples, demonstrations and/or testing must be provided within 7 calendar days of City's request. Failure to comply with City's request may result in rejection of a proposal. All samples (including return thereof), demonstrations, and/or

testing shall be at Respondent's expense. Samples will be returned upon written request. Requests for return of samples must be made in writing at the time the samples are provided. Otherwise, samples will become property of City at no cost to City. Samples that are consumed or destroyed during demonstrations or testing will not be returned.

Estimated Quantities for Annual Contracts.

Designation as an "annual" contract is found in the contract's title on the Cover Page of this document. The quantities stated are estimates only and are in no way binding upon City. Estimated quantities are used for the purpose of evaluation. City may increase or decrease quantities as needed. Where a contract is awarded on a unit price basis, payment shall be based on the actual quantities supplied.

Respondent's Due Diligence.

Respondents shall thoroughly examine the drawings, specifications, schedule(s), instructions and all other contract documents.

Respondents shall make all investigations necessary to thoroughly inform themselves regarding plant and facilities for delivery of material and equipment, or conditions and sites/locations for providing goods and services as required by this RFCSP. No plea of ignorance by Respondent will be accepted as a basis for varying the requirements of City or the compensation to Respondent.

Confidential or Proprietary Information. All proposals become the property of City upon receipt and will not be returned. Any information deemed to be confidential by Respondent should be clearly noted; however, City cannot guarantee that it will not be compelled to disclose all or part of any public record under the Texas Public Information Act, since information deemed to be confidential by Respondent may not be considered confidential under Texas law, or pursuant to a Court order.

Interlocal Participation.

City may engage in cooperative purchasing with other governmental entities or governmental cooperatives ("Entity" or "Entities") to enhance City's purchasing power. At City's sole discretion and option, City may inform other Entities that they may acquire items listed in this RFCSP. If this contract will be subject to cooperative purchasing, such fact will be indicated in the Supplemental Terms and Conditions portion of this RFCSP. Such acquisition(s) shall be at the prices stated in the proposal and shall be subject to Respondent's acceptance. Entities desiring to acquire items listed in this RFCSP shall be listed on a rider attached hereto, if known at the time of issuance of the RFCSP. City may issue subsequent riders after contract award setting forth additional Entities desiring to utilize this proposal.

Respondent must sign and submit the rider, if attached to this RFCSP, with its proposal, indicating whether Respondent wishes to allow other Entities to use its proposal. Respondent shall sign and return any subsequently issued riders within ten calendar days of receipt. Respondent's decision on whether to allow other Entities to use the proposal shall not be a factor in awarding this RFCSP.

Costs of Proposing. Respondent shall bear any and all costs that are associated with the preparation of the Proposal, attendance at the Pre-Submittal conference, if any, or during any phase of the selection process.

Rejection of Proposals.

City may reject any and all proposals, in whole or in part, cancel the RFCSP and reissue the solicitation. City may reject a proposal if:

Respondent misstates or conceals any material fact in the proposal; or

The proposal does not strictly conform to law or the requirements of the solicitation;

The proposal is conditional; or

Any other reason that would lead City to believe that the proposal is non-responsive or Respondent is not responsible.

City, in its sole discretion, may also waive any minor informalities or irregularities in any proposal, such as failure to submit sufficient proposal copies, failure to submit literature or similar attachments, or business affiliation information.

Variances and Exceptions to Proposal Terms. In order to comply with State law, respondents must submit proposals on the same material terms and conditions. Proposals that contain material variances or exceptions to the terms and conditions, including additional terms and conditions, will be rejected.

Changes to Proposal Form. Proposals must be submitted on the forms furnished, where forms are provided. Proposals that change the format or content of City's RFCSP will be rejected.

Withdrawal of Proposals. Proposals may be withdrawn prior to the due date for submission. Proposals submitted electronically may be withdrawn electronically.

Proposal Opening. The names of the respondents will be publicly read aloud online through WebEx at 2:30 P.M. Central Time on the day the proposals are due. In accordance with state law, the contents will not be revealed until after the contract is awarded.

Join by phone: 1-415-655-0001
Meeting number (access code): 177 587 8554

Evaluation and Award of Contract.

Per Section §252.043 of the Texas Local Government Code, the contract will be awarded to the responsible offeror whose proposal is determined to be the most advantageous to City, considering the relative importance of price and the other evaluation factors included in this RFCSP.

City reserves the right to evaluate pricing on the basis of low line item, low total line items, or in any other combination that serves the best interest of City, unless City designates this solicitation as an "all or none" proposal in the Supplemental Terms & Conditions.

A written award of acceptance (manifested by a City Ordinance) and Purchase Order furnished to Respondent results in a binding contract without further action by either party. City shall not be liable for any costs, claims, fees, expenses, damages, or lost profits if no Purchase Order is issued.

City reserves the right to utilize historical usage data as a basis for evaluation of proposals when future usages are unable to be determined.

City reserves the right to delete items prior to the awarding of the contract, and purchase said items by other means.

Inspection of Facilities/Equipment.

Depending on the nature of the RFCSP, Respondent's facilities and equipment may be a determining factor in making the proposal award. All respondents may be subject to inspection of their facilities and equipment.

Prospective respondents must prove beyond any doubt to City that they are qualified and capable of performing the contract's requirements.

Prompt Payment Discount.

Provided Respondent meets the requirements stated herein, City shall take Respondent's offered prompt payment discount into consideration. The evaluation will not be based on the discount percentage alone, but rather the net price as determined by applying the discount to the proposal price, either per line item or total proposal amount. However, City reserves the right to reject a discount if the percentage is too low to be of value to City, all things considered. City may also reject a discount if the percentage is so high as to create an overly large disparity between the price City would pay if it is able to take advantage of the discount and the price City would pay if it were unable to pay within the discount period. City may always reject the discount and pay within the 30 day period, at City's sole option.

City will not consider discounts that provide fewer than 10 days to pay in order to receive the discount.

For example, payment terms of 2% 5, Net 30 will NOT be considered in proposal evaluations or in the payment of invoices. However, payment terms of 2% 10, Net 30 will result in a two percent reduction in the proposal price during proposal evaluation, and City will take the 2% discount if the invoice is paid within the 10-day time period.

Prohibited Financial Interest.

The Charter of the City of San Antonio and the City of San Antonio Code of Ethics prohibit a City officer or employee, as those terms are defined in §§ 2-42 and 2-52 of the Code of Ethics, from having a direct or indirect financial interest in any contract with City. An officer or employee has a "prohibited financial interest" in a contract with City or in the sale to City of land materials, supplies or service, if any of the following individual(s) or entities is a party to the contract or sale:

- A City officer or employee; his or her spouse, sibling, parent, child, or other family member within the first degree of consanguinity or affinity;
- An entity in which the officer or employee, or his or her parent, child or spouse directly or indirectly owns (i) 10% or more of the voting stock or shares of the entity, or 10% or more of the fair market value of the entity; or
- An entity in which any individual or entity listed above is (i) a subcontractor on a City contract, (ii) a partner or (iii) a parent or subsidiary entity.

By submitting a bid, Bidder warrants and certifies, and a contract awarded pursuant to this RFCSP is made in reliance thereon, that it, its officers, employees and agents are neither officers nor employees of the City.

Unfair Advancement of Private Interests. Pricing and discounts contained in this contract are for use by City departments conducting City business. City employees may not use their positions to obtain special treatment or prices that are not available to the general public.

State of Texas Conflict of Interest.

Questionnaire (Form CIQ). Chapter 176 of the Texas Local Government Code requires that persons, or their agents, who seek to contract for the sale or purchase of property, goods, or services with the City, shall file a completed Form CIQ with the City Clerk if those persons meet the requirements under §176.006(a) of the statute.

By law this questionnaire must be filed with the City Clerk not later than the 7th business day after the date the vendor becomes aware of facts that require the statement to be filed. *See* Section 176.006(a-1), Texas Local Government Code.

Form CIQ is available from the Texas Ethics Commission by accessing the following web address:

https://www.ethics.state.tx.us/forms/conflict/

In addition, please complete the **City's Addendum to Form CIQ (Form CIQ-A)** and submit it with Form CIQ to the Office of the City Clerk. The Form CIQ-A can be found at:

http://www.sanantonio.gov/atty/ethics/pdf/OCC-CIQ-Addendum.pdf

When completed, the CIQ Form and the CIQ-A Form should be submitted together by mail to the Office of the City Clerk. Please mail to:

Office of the City Clerk, P.O. Box 839966, San Antonio, TX 78283-3966.

Do not include these forms with your sealed bid. The Purchasing Division will not deliver the forms to the City Clerk for you.

PART B

SUBMISSION REQUIREMENTS

Respondent's Proposal shall include the following items in the following sequence, noted with the appropriate heading as indicated below. If Respondent is proposing as a team or joint venture, provide the same information for each member of the team or joint venture.

Respondent shall limit any reference to the Respondent's proposed price to the respective section designated for this information. PLACING PRICE INFORMATION IN OTHER SECTIONS OF A RESPONSE TO THIS RFCSP MAY RESULT IN THE RESPONDENT'S PROPOSAL BEING DEEMED NON-RESPONSIVE AND THEREFORE DISQUALIFIED FROM CONSIDERATION.

TABLE OF CONTENTS

EXECUTIVE SUMMARY. The summary shall include a statement of the work to be accomplished, how Respondent proposes to accomplish and perform each specific service and unique problems perceived by Respondent and their solutions.

GENERAL INFORMATION FORM. Use the Form found in this RFCSP as Attachment A, Part One.

EXPERIENCE, BACKGROUND & QUALIFICATIONS. Use the Form found in this RFCSP as Attachment A, Part Two.

PROPOSED PLAN. Use the Form found in this RFCSP as Attachment A, Part Three.

PRICE SCHEDULE. Use the Price Schedule that is found in this RFCSP as Attachment B.

CONTRACTS DISCLOSURE FORM. Complete and submit a Contracts Disclosure Form with the proposal. The Contracts Disclosure Form may be downloaded at:

- Link to complete form electronically: https://webapp1.sanantonio.gov/ContractsDisclosure/
- Link to access PDF form to print and handwrite information: https://www.sanantonio.gov/portals/0/files/clerk/ethics/ContractsDisclosure.pdf

1. Download form and complete all fields. All fields must be completed prior to submitting the form.

2. All Respondents must include the following information in the required Contracts Disclosure Form at the time the original proposal is submitted:
   a. names of the agency board members and executive committee members,
   b. list of positions they hold as an individual or entity seeking action on any matter listed:
      (1) The identity of any individual who would be a party to the transaction;
      (2) The identity of any entity that would be a party to the transaction and the name of:
         a. Any individual or entity that would be a subcontractor to the transaction;
         b. Any individual or entity that is known to be a partner or a parent entity of any individual or entity who would be a party to the transaction, or any subsidiary entity that is anticipated to be involved in the execution of the transaction; and
         c. The board members, executive committee members, and officers of entities listed above; and
      (3) The identity of any lobbyist, attorney or consultant employed for purposes relating to the transaction being sought by any individual or entity who would be a party to the transaction.
   c. names and titles of officers of the organization.

3. Click on the “Print” button and place the copy in proposal response as indicated in the Proposal Checklist.

LITIGATION DISCLOSURE FORM. Complete and submit the Litigation Disclosure Form, found in this RFCSP as Attachment C. If Respondent is proposing as a team or joint venture, then all persons or entities who will be parties to the contract (if awarded) shall complete and return this form.

VETERAN–OWNED SMALL BUSINESS (VOSB) PROGRAM TRACKING FORM. Pursuant to Ordinance No. 2013-12-05-0864, all solicitations issued by the City are subject to tracking of Veteran Owned Small Business (VOSB) participation. For more information on the program, refer to the Veteran-Owned Small Business Program Tracking Form attached to this solicitation. Respondent must complete and return the attached Veteran-Owned Small Business Program Tracking Form with the proposal submitted, as Attachment D.

CERTIFICATE OF INTERESTED PARTIES (FORM 1295).

The Texas Government Code §2252.908, and the rules issued by the Texas Ethics Commission found in Title 1, Chapter 46 of the Texas Administrative Code, require a business entity to submit a completed Form 1295 to the City before the City may enter into a contract with that business entity.

Form 1295 must be completed online. It is available from the Texas Ethics Commission by accessing the following web address:

https://www.ethics.state.tx.us/filinginfo/1295

Print your completed Form 1295. Submit your signed Form 1295 with your response to this solicitation. Where requested to provide the name of the public entity with whom you are contracting, insert "City of San Antonio". Where requested to provide the contract number, provide the solicitation number shown on the cover page of this solicitation (e.g. IFB 6100001234, RFO 6100001234 or RFCSP 6100001234).

The following definitions found in the statute and Texas Ethics Commission rules may be helpful in completing Form 1295.

"Business entity" includes an entity through which business is conducted with a governmental entity or state agency, regardless of whether the entity is a for-profit or nonprofit entity. The term does not include a governmental entity or state agency. (NOTE: The City of San Antonio should never be listed as the "Business entity".)

"Controlling interest" means: (1) an ownership interest or participating interest in a business entity by virtue of units, percentage, shares, stock, or otherwise that exceeds 10 percent; (2) membership on the board of directors or other governing body of a business entity of which the board or other governing body is composed of not more than 10 members; or (3) service as an officer of a business entity that has four or fewer officers, or service as one of the four officers most highly compensated by a business entity that has more than four officers. Subsection (3) of this section does not apply to an officer of a publicly held business entity or its wholly owned subsidiaries.

"Interested party" means: (1) a person who has a controlling interest in a business entity with whom a governmental entity or state agency contracts; or (2) an intermediary.

"Intermediary," for purposes of this rule, means a person who actively participates in the facilitation of the contract or negotiating the contract, including a broker, adviser, attorney, or representative of or agent for the business entity who:

(1) receives compensation from the business entity for the person's participation;

(2) communicates directly with the governmental entity or state agency on behalf of the business entity regarding the contract; and

(3) is not an employee of the business entity or of an entity with a controlling interest in the business entity.

Publicly traded business entities, including their wholly owned subsidiaries, are exempt from this requirement and are not required to submit Form 1295.

PROOF OF INSURABILITY. Submit a letter from insurance provider stating provider's commitment to insure the Respondent for the types of coverages and at the levels specified in this RFCSP if awarded a contract in response to this RFCSP. Respondent shall also submit a copy of their current insurance certificate.

FINANCIAL INFORMATION**.** Submit a recent copy of a Dun and Bradstreet financial report, or another credit report, on Respondent and its partners, affiliates, and subtenants, if any.

THIRD PARTY VENDOR IT CLOUD SECURITY QUESTIONNAIRE. If a Software as a Service (SaaS) solution is proposed, the respondent will be required to complete the appropriate Third-Party Vendor IT Cloud Security Questionnaire provided under Attachment G.

SIGNATURE PAGE. Respondent must complete, sign and submit the Signature Page found in this RFCSP Section 007. The Signature Page must be signed by a person, or persons, authorized to bind the entity, or entities, submitting the proposal. Proposals signed by a person other than an officer of a corporate respondent or partner of partnership respondent shall be accompanied by evidence of authority.

PROPOSAL CHECKLIST. Complete and submit the Proposal Checklist found in this RFCSP as Attachment K.

ADDENDA. Sign and submit addenda, if any.

Respondent is expected to examine this RFCSP carefully, understand the terms and conditions for providing the services listed herein and respond completely. FAILURE TO COMPLETE AND PROVIDE ANY OF THESE PROPOSAL REQUIREMENTS MAY RESULT IN THE RESPONDENT'S PROPOSAL BEING DEEMED NON-RESPONSIVE AND THEREFORE DISQUALIFIED FROM CONSIDERATION.

EVALUATION CRITERIA

The City will conduct a comprehensive, fair and impartial evaluation of all submissions received in response to this RFCSP. The City may appoint a selection committee to perform the evaluation. Each submission will be analyzed to determine overall responsiveness and qualifications under this RFCSP. Criteria to be evaluated will include the items listed below. The selection committee may select respondents who are judged to be reasonably qualified for interviews, depending on whether further information is needed. Interviews are not an opportunity to change a submission. If the City elects to conduct interviews, respondents may be interviewed and re-scored based upon the same criteria. City may also request information from respondents at any time prior to final approval of a selected respondent or seek best and final offers from respondents deemed reasonably qualified for award. Final approval of a selected respondent is subject to the action of the San Antonio City Council.

Evaluation Criteria:

Experience, Background, Qualifications (40 points)

Proposed Plan (40 points)

Price (20 points)

004 - SPECIFICATIONS / SCOPE OF SERVICES

Background

The City of San Antonio Aviation (hereafter referred to as "Aviation") is seeking proposals from qualified firms interested in providing a web hosted ground transportation software solution that will independently track the activities of Application based ground transportation providers, Transportation Network Companies (TNCs) doing business in and around the San Antonio International Airport (SAIA) property. The City is currently utilizing the TNC-OPS solution provided by Gatekeeper Systems. Here is a link to their product: https://gksys.com/airport-software-products/tnc-ops/

Qualified Respondent shall demonstrate prior or similar design experience with a functioning installation of a web hosted ground transportation software solution at three larger or similar sized airports having similar TNC activities. Respondent shall possess the range of design and project management expertise required to plan and design the Project within the context of a complex airport environment.

TNCs utilize independently owned and web-based applications to arrange rides between customers and independent drivers working for them. SAIA would like a third-party software application to independently retrieve and process data from all TNCs permitted by the City of San Antonio.

The Application-Based Commercial Ground Transportation (ABCT) software will need to provide real-time data transactions, demographic on vehicles, and fees from all TNCs conducting business at SAIA. The selected Respondent's solution must be accessible either by desktop or mobile devices.

Aviation, with the assistance of the Respondent, will establish a "Geo-Fence" within airport property. The term "Geo-Fence" is a polygon whose points are geographic coordinates on Airport property designated by the Airport (as may be amended by the Airport from time to time) pursuant to the Airport's ABCT Permits with Designated ABCT Providers.

The selected Respondent will not and cannot be responsible for the invoicing and collection of fees from a TNC provider. Aviation will independently make those arrangements and will be responsible for auditing self-reports from the TNC Providers to the data obtained from the Respondent's software solution.

Selected Respondent will provide all implementation and configuration to include testing, training and all documentation needed.

Definitions – In addition to Section 008 – Standard Definitions:

a) **San Antonio Airport Systems** – further referred to as "SAAS" shall mean the San Antonio International Airport, the Stinson Municipal Airport and any other property that is added to or associated with the Airport System.

b) **San Antonio International Airport** – further referred to as "SAT" or "Airport"

c) **Geo-Fence** - Is a polygon whose points are geographic coordinates which define a virtual boundary around a geographic area on SAT property designated by SAT. There may be multiple Geo fences that are nested or geographically separate from the main fence surrounding the entire Airport property.

d) **TNC or Transportation Network Company** - means a corporation, partnership, sole proprietorship, or other entity operating in Texas that uses a digital network to connect a transportation network company rider to a transportation network company driver for a prearranged ride. The term does not include an entity arranging nonemergency medical transportation under a contract with the state or a managed care organization for individuals qualifying for Medicaid or Medicare.

e) **TNC Driver** – means an individual who (i) receives connections to potential Transportation Network Company riders and related services from a Transportation Network Company in exchange for payment of a fee to the company; and (ii) uses a personal vehicle to offer or provide a prearranged ride to a Transportation Network Company rider. For purposes of this Agreement, TNC Driver refers to a TNC Driver operating on Licensee's platform.

f) **Trips** – any instance in which a TNC Driver enters Airport property (as defined by the geo fence(s)) and makes one or more stops to pick-up one or more passengers.

Scope of Services

This Scope of Work is to be used as a general guide and is not intended to be a complete list of all work necessary to complete the project.

The selected Respondent shall track all TNC vehicles at various stages based on transaction type described below. For each transaction type, the Respondent's software shall capture the following transaction type information, including but not limited to: date, time, geographical location, TNC identification, TNC Driver based unique identifier and vehicle license plate number.

Tracking of TNC Endorsed Vehicles –

A. For each "TNC Driver," the Respondent's ABCT software solution shall be capable of obtaining, in "real time", the following "Required Data" upon each of the "Triggering Events."

1. **Required Data**:
   a) Transaction type (i.e., entry, exit, drop-off, pick-up)
   b) TNC Provider identification
   c) Date
   d) Time
   e) Geographical location (for all exits and entries)
   f) Unique driver identifier
   g) Vehicle license plate number
   h) Number of active rides in the vehicle following the triggering event [based on a value of "0" (no active rides) or "1" (active ride)]

2. **Triggering Events**:
   a) Upon entry into the Geo-Fence
   b) Upon completion of a passenger drop-off within the Geo-Fence (other geo fencing on property)
   c) Upon pick-up of a passenger within Geo-Fence
   d) Upon exit of Geo-Fence

B. **Upon Entry**: Upon entry into the Geo-Fence, TNC company shall electronically notify ("ping") selected Respondent, in real time with the unique identifier and license plate number of each TNC Vehicle, including date, time, geographical location, TNC identification, driver-based unique identifier, vehicle license plate number and the number of active TNC rides in the vehicle at the time of entry. The ping shall be transmitted by TNC Company to the selected Respondent at the moment each TNC Vehicle crosses the Geo-Fence.

C. **Upon Ride Completion (on Airport property)**: When the TNC Driver completes a drop-off trip by indicating on his or her smart phone app that the ride is complete, TNC Company shall instantaneously send a second ping to the selected Respondent, including date, time, geographical location, TNC identification, driver-based unique identifier, vehicle license plate number and the number of active TNC rides remaining in the TNC Vehicle following ride completion.

D. **Upon Passenger Pick-Up (on Airport property):** When the TNC Driver picks up a passenger on Airport property by indicating on his or her smart phone app that a passenger has been picked up, TNC Company shall instantaneously send a ping to the selected Respondent, including date, time, geographical location, TNC identification, driver-based unique identifier, vehicle license plate number and the number of active TNC rides remaining in the TNC Vehicle following passenger pick up.

E. **Exiting the Geo-Fence:** Upon exiting the Geo-Fence, TNC Company shall instantaneously send a final ping to the selected Respondent, including date, time, geographical location, TNC identification, driver-based unique identifier, vehicle license plate number and the number of active TNC rides remaining in the TNC Vehicle following passenger pick up.

F. **Reports:** Selected Respondent software should be able to provide reporting on all transactions and provide historical reports. Selected Respondent shall keep all data for a minimum of 4 years. Reports should be in an electronic form approved by the Aviation.

License – Respondent shall grant City a paid-up, non-exclusive, non-transferable license for the software / use of the Services, including maintenance and support services, for the Original Contract Term and for the Renewals periods, if exercised by City.

005 - SUPPLEMENTAL TERMS & CONDITIONS

Original Contract Term:

This contract shall begin upon the effective date of the ordinance awarding the contract or January 1, 2023, whichever is later. This contract shall begin upon the date specified in the award letter, if it does not exceed $50,000. The contract shall terminate on December 31, 2025.

Renewals:

At City's option, this Contract may be renewed under the same terms and conditions for two (2) additional (1) year period(s). Renewals shall be in writing and signed by Director, without further action by the San Antonio City Council, subject to and contingent upon appropriation of funding therefore.

Temporary Short-Term Extensions.

City shall have the right to extend this contract under the same terms and conditions beyond the original term or any renewal thereof, on a month to month basis, not to exceed three months. Said month to month extensions shall be in writing, signed by Director, and shall not require City Council approval, subject to and contingent upon appropriation of funding therefore.

Temporary Contract Pending Award of Contract by City Council

Occasionally, the City has a need for goods or services prior to the date set for the San Antonio City Council to consider a contract for award. If such a situation arises with regard to this solicitation, and if City intends to recommend Vendor's bid to the City Council for award of a contract, City may require Vendor to provide goods or services prior to the date set for City Council to consider the bid for award of a contract. City shall provide Vendor advance written notice if such occasion arises.

In such event, City's written notice shall constitute acceptance of Vendor's bid and shall result in a temporary contract to provide goods and/or services until City Council considers and awards the contract contemplated in this solicitation. The total expenditure under the temporary contract shall not exceed $50,000. The temporary contract shall begin on the date set forth in City's written notice and shall terminate when the total expenditure reaches $50,000, or upon subsequent written notice from City, whichever shall occur sooner. Should City Council authorize award of a contract to Vendor pursuant to this solicitation, said award shall automatically terminate the temporary contract upon the effective date of the newly awarded contract.

During the term of the temporary contract, all goods or services shall be provided in accordance with the terms and conditions contained in this solicitation, with the exception of the Original Contract Term, which is modified as indicated above for the temporary contract.

Acceptance of Vendor's bid for the purposes of award of a temporary contract does not constitute award of the full contract with the Original Contract Term. Such a contract may only be awarded by the San Antonio City Council by passage of an ordinance. Neither does award of a temporary contract obligate City to recommend Vendor's bid for award to the City Council or guarantee that the City Council will award the contract to Vendor.

Internal / External Catalog.

San Antonio e-Procurement. The City is using an "e-Procurement" system (SAePS) based on SAP's Supplier Relationship Management (SRM) software. SAePS is a secure, web browser-based system that gives City employees the ability to shop for items from online catalogs and brings the items back automatically into SAePS. Online catalogs include both a SAePS internal catalog and externally hosted catalogs on supplier websites.

SAePS Electronic Catalog Options. Vendor shall furnish an electronic catalog that contains only the items awarded by City and displays pricing proposed under this contract. Vendor may choose either Option 1 or Option 2 below as the method for furnishing the catalog.

Option 1. Vendor shall host an online catalog (Punch Out Catalog) with Open Catalog Interface (OCI) compliant integration to the SAePS system. This Punch Out Catalog shall have e-commerce functions, including, but not limited to, cataloging, searching and shopping cart functionality. Integration includes linking to the online catalog from SAePS, shopping, and electronically returning the data back to SAePS.

Option 2. Internal Catalog. Vendor shall provide a list of products and services awarded under this contract for uploading into the COSA e-Procurement system in an electronic format as specified by City. The electronic submission may be through email, unless it exceeds City's maximum allowable file size limit. In such case, Vendor shall provide the submission on a CD or other means approved by City.

Paper Catalog. If a Punch Out Catalog is not available and Vendor elects to provide an Internal Catalog, City, at its sole option, may require Vendor to provide its Internal Catalog in paper form in addition to the electronic form.

Catalog Content. All catalogs, regardless of the form in which they are provided, must include these elements, at a minimum.

- Your part numbers
- Short and long descriptions
- Units of measure
- Pricing, contract pricing, tiered pricing
- Classification of parts
- Manufacturer and Manufacturer part number
- Keywords, tags

Time to Provide Catalog. Catalogs required under this provision must be provided within 10 business days of request by City, and no later than 5 business days from the date of contract award.

Catalog Updates.
If this contract allows for increases in price, Vendor must provide timely updates to the City. For Punch Out catalogs, Vendor must update pricing on their website and provide City a notification and detailed explanation of the price updates. For Internal Catalogs, Vendor must provide an updated pricing file with details of the pricing updates. If paper catalogs have been requested, updated paper catalogs must be provided concurrently with Internal Catalog files, or as soon thereafter as printed catalogs become available.

Insurance

A) Prior to the commencement of any work under this Agreement, Respondent shall furnish copies of all required endorsements and completed Certificate(s) of Insurance to the City's Aviation Department, which shall be clearly labeled **"*Rideshare Monitoring Services for San Antonio International Airport*"** in the Description of Operations block of the Certificate. The Certificate(s) shall be completed by an agent and signed by a person authorized by that insurer to bind coverage on its behalf. The City will not accept a Memorandum of Insurance or Binder as proof of insurance. The certificate(s) must have the agent's signature and phone number, and be mailed, with copies of all applicable endorsements, directly from the insurer's authorized representative to the City. The City shall have no duty to pay or perform under this Agreement until such certificate and endorsements have been received and approved by the City's Aviation Department. No officer or employee, other than the City's Risk Manager, shall have authority to waive this requirement.

B) The City reserves the right to review the insurance requirements of this Article during the effective period of this Agreement and any extension or renewal hereof and to modify insurance coverages and their limits when deemed necessary and prudent by City's Risk Manager based upon changes in statutory law, court decisions, or circumstances surrounding this Agreement. In no instance will City allow modification whereby City may incur increased risk.

C) A Respondent's financial integrity is of interest to the City; therefore, subject to Respondent's right to maintain reasonable deductibles in such amounts as are approved by the City, Respondent shall obtain and maintain in full force and effect for the duration of this Agreement, and any extension hereof, at Respondent's sole expense,

insurance coverage written on an occurrence basis, unless otherwise indicated, by companies authorized to do business in the State of Texas and with an A.M Best's rating of no less than A- (VII), in the following types and for an amount not less than the amount listed below:

TYPE	AMOUNTS
1. Workers' Compensation 2. Employers' Liability	Statutory $1,000,000/$1,000,000/$1,000,000
3. Commercial General Liability Insurance to include coverage for the following: a. Premises/Operations b. Products/Completed Operations c. Personal/Advertising Injury d. Contractual Liability e. Independent Contractors	For Bodily Injury and Property Damage of $1,000,000 per occurrence; $2,000,000 General Aggregate, or its equivalent in Umbrella or Excess Liability Coverage
4. Professional Liability	$1,000,000 per claim damages by reason of any act, malpractice, error, or omission in the professional service. *Coverage to be maintained and in effect for no less than two years subsequent to the completion of the professional service.
*5. Cyber Liability	$1,000,000 per claim $2,000,000 general aggregate, or its equivalent in Umbrella or Excess Liability Coverage.
6. Business Automobile Liability a. Owned/leased vehicles b. Non-owned vehicles c. Hired Vehicles	Combined Single Limit for Bodily Injury and Property Damage of $1,000,000 per occurrence. **If AOA access $5,000,000 CSL**.
*If Applicable	

D) Respondent agrees to require, by written contract, that all subcontractors providing goods or services hereunder obtain the same insurance coverages required of Respondent herein and provide a certificate of insurance and endorsement that names the Respondent and the CITY as additional insureds. Respondent shall provide the CITY with said certificate and endorsement prior to the commencement of any work by the subcontractor. This provision may be modified by City's Risk Manager, without subsequent City Council approval, when deemed necessary and prudent, based upon changes in statutory law, court decisions, or circumstances surrounding this agreement. Such modification may be enacted by letter signed by City's Risk Manager, which shall become a part of the contract for all purposes.

E) As they apply to the limits required by the City, the City shall be entitled, upon request and without expense, to receive copies of the policies, declaration page, and all endorsements thereto and may require the deletion, revision, or modification of particular policy terms, conditions, limitations, or exclusions (except where policy provisions are established by law or regulation binding upon either of the parties hereto or the underwriter of any such policies). Respondent shall be required to comply with any such requests and shall submit a copy of the replacement certificate of insurance to City at the address provided below within 10 days of the requested change. Respondent shall pay any costs incurred resulting from said changes.

City of San Antonio
Attn: Aviation Department – Parking and Ground Transportation
P.O. Box 839966
San Antonio, Texas 78283-3966

F) Respondent agrees that with respect to the above required insurance, all insurance policies are to contain or be endorsed to contain the following provisions:

- Name the City, its officers, officials, employees, volunteers, and elected representatives as additional insureds by endorsement, as respects operations and activities of, or on behalf of, the named insured

performed under contract with the City, with the exception of the workers' compensation and professional liability policies;

- Provide for an endorsement that the "other insurance" clause shall not apply to the City of San Antonio where the City is an additional insured shown on the policy;

- Workers' compensation, employers' liability, general liability and automobile liability policies will provide a waiver of subrogation in favor of the City.

- Provide advance written notice directly to City of any suspension, cancellation, non-renewal or material change in coverage, and not less than ten (10) calendar days advance notice for nonpayment of premium.

G) Within five (5) calendar days of a suspension, cancellation or non-renewal of coverage, Respondent shall provide a replacement Certificate of Insurance and applicable endorsements to City. City shall have the option to suspend Respondent's performance should there be a lapse in coverage at any time during this contract. Failure to provide and to maintain the required insurance shall constitute a material breach of this Agreement.

H) In addition to any other remedies the City may have upon Respondent's failure to provide and maintain any insurance or policy endorsements to the extent and within the time herein required, the City shall have the right to order Respondent to stop work hereunder, and/or withhold any payment(s) which become due to Respondent hereunder until Respondent demonstrates compliance with the requirements hereof.

I) Nothing herein contained shall be construed as limiting in any way the extent to which Respondent may be held responsible for payments of damages to persons or property resulting from Respondent's or its subcontractors' performance of the work covered under this Agreement.

J) It is agreed that Respondent's insurance shall be deemed primary and non-contributory with respect to any insurance or self-insurance carried by the City of San Antonio for liability arising out of operations under this Agreement.

K) It is understood and agreed that the insurance required is in addition to and separate from any other obligation contained in this Agreement and that no claim or action by or on behalf of the City shall be limited to insurance coverage provided.

L) Respondent and any Subcontractors are responsible for all damage to their own equipment and/or property.

Undisclosed Features. Vendor warrants that the code and software provided to the City of San Antonio under this agreement does not contain any undisclosed features or functions that would impair or might impair the City's use of the equipment, code or software. Specifically, but without limiting the previous representation, Vendor warrants there is no "Trojan Horse," lock, "time bomb," backdoor or similar routine. This Agreement shall not now nor will it hereafter be subject to the self-help provisions of the Uniform Computer Information Transactions Act or any other law. Vendor specifically disclaims any unilateral self-help remedies.

Intellectual Property.

Vendor shall pay all royalties and licensing fees. Vendor shall hold the City harmless and indemnify the City from the payment of any royalties, damages, losses or expenses including attorney's fees for suits, claims or otherwise, growing out of infringement or alleged infringement of copyrights, patents, trademarks, trade secrets, materials and methods used in the project. It shall defend all suits for infringement of any Intellectual Property rights. Further, if Vendor has reason to believe that the design, service, process or product specified is an infringement of an Intellectual Property right, it shall promptly give such information to the City.

Upon receipt of notification that a third-party claims that the program(s), hardware or both the program(s) and the hardware or any other intellectual property infringe upon any United States or International patent, copyright or trademark, Vendor will immediately:

Obtain, at Vendor's sole expense, the necessary license(s) or rights that would allow the City to continue using the programs, hardware, both the programs and hardware or any other intellectual property as the case may be, or

Alter the programs, hardware, or both the programs and hardware so that the alleged infringement is eliminated; and

Reimburse the City for any expenses incurred by the City to implement emergency backup measures if the City is prevented from using the programs, hardware, or both the programs and hardware while the dispute is pending.

Vendor further agrees to

assume the defense of any claim, suit, or proceeding brought against the City for infringement of any United States patent, copyright, trademark or any other intellectual property rights arising from the use and/or sale of the equipment or software under this Agreement,

assume the expense of such defense, including costs of investigations, reasonable attorneys' fees, expert witness fees, damages, and any other litigation-related expenses, and

indemnify the City against any monetary damages and/or costs awarded in such suit;

provided that

Vendor is given sole and exclusive control of all negotiations relative to the settlement thereof, but that Vendor agrees to consult with the City Attorney of the City during such defense or negotiations and make good faith effort to avoid any position adverse to the interest of the City,

the Software or the equipment is used by the City in the form, state, or condition as delivered by Vendor or as modified without the permission of Vendor, so long as such modification is not the source of the infringement claim,

the liability claimed shall not have arisen out of the City's negligent act or omission, and

the City promptly provide Vendor with written notice within 15 days following the formal assertion of any claim with respect to which the City asserts that Vendor assumes responsibility under this section.

Incorporation of Attachments.

In connection with the services being provided, Vendor may need to operate certain information technology systems not owned by the City (Non-City Systems), which may need to interface with or connect to City's networks, internet access, or information technology systems (City Systems). Vendor shall be responsible for all Non-City Systems, and City shall be solely responsible for City Systems, including taking the necessary security and privacy protections as are reasonable under the circumstances. Vendor agrees to comply with all applicable City Administrative Directives, including but not limited to, Administrative Directive (AD) 7.4A, Acceptable Use of Information Technology, AD 7.8d, Access Control, and AD 7.3a, Data Security.

Each of the attachments listed below is an essential part of this contract, which governs the rights and duties of the parties, incorporated herein by reference, and shall be interpreted in the order of priority as appears below, with this document taking priority over all attachments:

Attachment A – Part One – General Information Form
Attachment A – Part Two – Experience, Background and Qualifications
Attachment A – Part Three – Proposed Plan
Attachment B – Price Schedule
Attachment C – Litigation Disclosure Form
Attachment D – Veteran Owned Small Business (VOSB) Preference Program Tracking Form
Attachment E – Mandatory Federal Provisions
Attachment F – Acceptable Use of Information Technology
Attachment G – Third Party Vendor IT Cloud Security Questionnaire
Attachment H – Access Control
Attachment I – Data Security
Attachment J – Pre-Submittal Conference Agenda
Attachment K – Proposal Checklist
Attachment L – Pre-Submittal Conference Sign-In Sheet.

006 - GENERAL TERMS & CONDITIONS

Electronic Proposal Equals Original. If Vendor is submitting an electronic proposal, City and Vendor each agree that this transaction may be conducted by electronic means, as authorized by Chapter 322, Texas Business & Commerce Code, known as the Electronic Transactions Act.

Delivery of Goods/Services.

Destination Contract. Vendor shall deliver all goods and materials F.O.B., City of San Antonio's designated facility, inside delivery, freight prepaid, to the address provided in this RFCSP or, if different, in the Purchase Order. Vendor shall bear the risk of loss until delivery. Freight charges will be paid only when expedited delivery is requested and approved in writing by the City. Vendor shall be responsible for furnishing necessary personnel or equipment and/or making necessary arrangements to off load at City of San Antonio facility, unless otherwise noted herein.

Failure to Deliver. When delivery is not met as provided for in the contract, the City may make the purchase on the open market, with any cost in excess of the contract price paid by Vendor, in addition to any other direct, indirect, consequential or incidental damages incurred by the City as a result thereof. In addition, Vendor may be removed from the City's list of eligible Respondents.

Purchase Orders. Each time a City department wishes to place an order against this contract, it will issue Vendor a purchase order. Vendor must have the purchase order before making any delivery.

Acceptance by City. City shall have a reasonable time (but not less than 30 days) after receipt to inspect the goods and services tendered by Vendor. City at its option may reject all or any portion of such goods or services which do not, in City's sole discretion, comply in every respect with all terms and conditions of the contract. City may elect to reject the entire goods and services tendered even if only a portion thereof is nonconforming. If the City elects to accept nonconforming goods and services, the City, in addition to its other remedies, shall be entitled to deduct a reasonable amount from the price thereof to compensate the City for the nonconformity. Any acceptance by the City, even if non-conditional, shall not be deemed a waiver or settlement of any defect in such goods and services.

Testing. After award of contract, City may, at its sole option, test the product delivered to ensure it meets specifications. Initial testing shall be at City's expense. However, if the product does not to meet specifications, Vendor shall reimburse City for the costs of testing. City may withhold the cost of testing from any amounts owed to Vendor under this or any other contract, or invoice Vendor for same. If invoiced, Vendor shall pay City within 30 calendar days' of the invoice.

Warranty. A minimum of 90-days product guarantee or the manufacturer's standard commercial warranty, whichever is greater, shall apply to all products and/or services purchased under this RFCSP, unless otherwise specified in the Specifications/Scope of Services section of this RFCSP. This warranty shall provide for replacement of defective merchandise, parts, and labor, and shall include pick-up of the defective merchandise from City and delivery of the replacement(s) to the same location. The warranty shall be effective from the date of acceptance of the merchandise, or completion of the service, as applicable.

REJECTION OF DISCLAIMERS OF WARRANTIES & LIMITATIONS OF LIABILITY. ANY TERM OR CONDITION IN ANY DOCUMENT FURNISHED BY VENDOR, DISCLAIMING THE IMPLIED WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE, OR ATTEMPTING TO LIMIT VENDOR'S LIABILITY SHALL BE OF NO FORCE OR EFFECT, AND SHALL BE STRICKEN FROM THE CONTRACT DOCUMENTS AS IF NEVER CONTAINED THEREIN.

Invoicing and Payment.

Invoice Submissions. City requires all original first-time invoices to be submitted directly to the Accounts Payable section of the Finance Department. The preferred method of delivery is electronically to the following e-mail address:

accounts.payable@sanantonio.gov

Invoices submitted electronically to the e-mail address above must be in separate .pdf format file. Multiple invoices cannot be submitted in a single .pdf file; however, Vendor may submit multiple, separate invoice files in a single e-mail. Any required documentation in support of the invoice should be compiled directly behind the invoice in the same .pdf file. Each electronically submitted file must have a unique identifying name that is not the same as any other file name.

Invoices submitted by electronic submission are only considered "original" when the submission comes directly from the Vendor to Accounts Payable using this e-mail address. Vendor may courtesy copy the ordering City department personnel on the e-mail.

Vendors not able to submit invoices with the required file formatting above may mail original invoices, on white paper only, to: City of San Antonio, Attn: Accounts Payable, P.O. Box 839976, San Antonio, Texas 78283-3976.

Information Required on Invoice.

All invoices must be in a form and content approved by the City. City may require modification of invoices if necessary in order to satisfy City that all billing is proper and pursuant to the terms of the contract. Invoices are required to show each City Purchase Order Number. Invoices must be legible. Items billed on invoices must be specific as to applicable stock, manufacturer, catalog or part number (if any). All invoices must show unit prices for each item being billed, the quantity of items being billed and the total for each item, as well as the total for all items on the invoice. If prices are based on list prices basis, then the list prices, the percentage discount or percentage surcharge, net unit prices, extensions and net total prices must be shown. Prompt payment discounts offered shall be shown separately on the invoice.

Payment by City.

In accordance with the Texas Prompt Payment Act, City shall have not less than 30 days to pay for goods or services. Time for payment, including payment under discount terms, will be computed from the later of: (1) the date the City receives conforming goods under the contract; (2) the date performance of the service under the contract is completed; or (3) the date the City receives a correct and valid invoice for the goods or services. Payment is deemed to be made on the date of mailing of the check. Payment is made in US dollars only.

This provision shall not apply where there is a bona fide dispute between the City and Vendor about the goods delivered or the service performed that causes the payment to be late, or where the invoice is not mailed to the address provided herein.

The payment amount due on invoices may not be manually altered by City personnel. Once disputed items are reconciled, Vendor must submit a corrected invoice or a credit memorandum for the disputed amount.

NECESSITY OF TIMELY INVOICE / WAIVER OF PAYMENT. NOTWITHSTANDING THE FORGOING, THE CITY CANNOT PAY FOR ANY GOODS OR SERVICES WITHOUT AN INVOICE. VENDOR MUST INVOICE CITY NO LATER THAN 90 CALENDAR DAYS FROM THE DATE GOODS ARE DELIVERED OR SERVICES RENDERED. FAILURE TO SUBMIT AN INVOICE WITHIN SAID 90 DAY SHALL NEGATE ANY LIABILITY ON THE PART OF CITY AND CONSTITUTE A **WAIVER** BY VENDOR OF ANY AND ALL RIGHT OR CLAIMS TO COLLECT MONEYS THAT VENDOR MAY RIGHTFULLY BE OTHERWISE ENTITLED TO FOR GOODS OR SERVICES PERFORMED.

The total price for all goods and/or services is shown on the Price Schedule. No additional fees or expenses of Vendor shall be charged by Vendor nor be payable by City. The parties hereby agree that all compensable expenses of Vendor are shown on the Price Schedule. If there is a discrepancy on the Price Schedule between the unit price for an item, and the extended price, the unit price shall govern. Unless otherwise provided in the Supplemental Terms and Conditions section of this document, all prices shown on the Price Schedule shall remain firm for the duration of the contract. Vendor's price stated on the Price Schedule shall be deemed a maximum price. Vendor may provide a lower price at any time during the contract period for reasons deemed appropriate by Vendor, such as volume discount pricing for large orders.

Change Orders. In order to comply with Texas law governing purchases made by municipalities, the following rules shall govern all change orders made under this contract.

Any change orders that become necessary during the term of this contract as a result of changes in plans, specifications, quantity of work to be performed, materials, equipment or supplies to be
must be in writing and conform to the requirements of City Ordinance 2011-12-08-1014, as hereafter amended.
Any other change will require approval of the City Council, City of San Antonio.

Changes that do not involve an increase in contract price may, however, be made by the Director.

No oral statement of any person shall modify or otherwise change, or affect the terms, conditions or specifications stated herein.

Termination.

Termination-Breach. Should Vendor fail to fulfill in a timely and proper manner, as determined solely by the Director, its material obligations under this contract, or violate any of the material terms of this contract, the City shall have the right to immediately terminate the contract in whole or in part. Notice of termination shall be provided in writing to Vendor, effective upon the date set forth in the notice. City may, in City's sole discretion, provide an opportunity for Vendor to cure the default. If City elects to offer an opportunity to cure, City shall provide notice to Vendor specifying the matters in default and the cure period. If Vendor fails to cure the default within the cure period, City shall have the right, without further notice, to terminate the contract in whole or in part. Such termination shall not relieve Vendor of any liability to the City for damages sustained by virtue of any breach by Vendor.

Termination-Notice. City may terminate this contract, in whole or in part, without cause. City shall be required to give Vendor notice ten days prior to the date of termination of the contract without cause.

Termination-Funding. City retains the right to terminate this contract at the expiration of each of City's budget periods. This contract is conditioned on a best efforts attempt by City to obtain and appropriate funds for payment of any debt due by City herein.

Termination by City may be effected by Director, without further action by the San Antonio City Council.

Independent Contractor. Vendor covenants and agrees that it is an independent contractor and not an officer, agent, servant or employee of City. City shall not be liable for any claims which may be asserted by any third party occurring in connection with the services to be performed by Vendor under this contract and that Vendor has no authority to bind City. The doctrine of respondeat superior shall not apply as between City and Vendor.

INDEMNIFICATION.

VENDOR covenants and agrees to FULLY INDEMNIFY, DEFEND and HOLD HARMLESS, CITY and the elected officials, employees, officers, directors, volunteers and representatives of CITY, individually and collectively, from and against any and all costs, claims, liens, damages, losses, expenses, fees, fines, penalties, proceedings, actions, demands, causes of action, liability and suits of any kind and nature, including but not limited to, personal or bodily injury, death and property damage, made upon the CITY directly or indirectly arising out of, resulting from or related to VENDOR'S activities under this Agreement, including any acts or omissions of VENDOR, any agent, officer, director, representative, employee, consultant or subcontractor of VENDOR, and their respective officers, agents employees, directors and representatives while in the exercise of the rights or performance of the duties under this Agreement. The indemnity provided for in this paragraph shall not apply to any liability resulting from the negligence of CITY, its officers or employees, in instances where such negligence causes personal injury, death, or property damage. IN THE EVENT VENDOR AND CITY ARE FOUND JOINTLY LIABLE BY A COURT OF COMPETENT JURISDICTION, LIABILITY SHALL BE APPORTIONED COMPARATIVELY IN ACCORDANCE WITH THE LAWS FOR THE STATE OF TEXAS, WITHOUT, HOWEVER, WAIVING ANY GOVERNMENTAL IMMUNITY AVAILABLE TO THE CITY UNDER TEXAS LAW AND WITHOUT WAIVING ANY DEFENSES OF THE PARTIES UNDER TEXAS LAW. In addition, Vendor agrees to indemnify, defend, and hold the City harmless from any claim involving patent infringement, trademarks, trade secrets, and copyrights on goods supplied.

The provisions of this INDEMNITY are solely for the benefit of the parties hereto and not intended to create or grant any rights, contractual or otherwise, to any other person or entity. VENDOR shall advise CITY in writing within 24 hours of any claim or demand against CITY or VENDOR known to VENDOR related to or arising out of VENDOR's activities under this AGREEMENT and shall see to the investigation and defense of such claim or demand at VENDOR's cost. CITY shall have the right, at its option and at its own expense, to participate in such defense without relieving VENDOR of any of its obligations under this paragraph.

Assignment. Except as otherwise stated herein, Vendor may not sell, assign, pledge, transfer or convey any interest in this contract, nor delegate the performance of any duties hereunder, by transfer, by subcontracting or any other means, without the consent of Director. As a condition of such consent, if such consent is granted, Vendor shall remain liable for completion of the services and provision of goods outlined in this contract in the event of default by the successor vendor, assignee, transferee or subcontractor. Any attempt to transfer, pledge or otherwise assign this Contract without said written approval, shall be void ab initio and shall confer no rights upon any third person.

Ownership of Documents. Pursuant to Texas Local Government Code Chapter 201, any and all Records produced by Vendor pursuant to the provisions of this contract are the exclusive property of City; and no such Record shall be the subject

of any copyright or proprietary claim by Vendor. The term "Record" as used herein shall mean any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium, or other information recording medium, regardless of physical form or characteristic. Vendor understands and acknowledges that as the exclusive owner of any and all such Records, City has the right to use all such Records as City desires, without restriction.

The requirements of Subchapter J, Chapter 552, Government Code, may apply to this contract and the contractor or vendor agrees that the contract can be terminated if the contractor or vendor knowingly or intentionally fails to comply with a requirement of that subchapter.

Records Retention.

Vendor and its subcontractors, if any, shall properly, accurately and completely maintain all documents, papers, and records, and other evidence pertaining to the services rendered hereunder ("Documents"), and shall make such Documents available to the City at their respective offices, at all reasonable times and as often as City may deem necessary during the contract period, including any extension or renewal hereof, and the record retention period established herein, for purposes of audit, inspection, examination, and making excerpts or copies of same by City and any of its authorized representatives.

Vendor shall retain any and all Documents produced as a result of services provided hereunder for a period of four years ("Retention Period") from the date of termination of the contract. If, at the end of the Retention Period, there is litigation or other questions arising from, involving or concerning these Documents or the services provided hereunder, Vendor shall retain the records until the resolution of such litigation or other such questions. Vendor acknowledges and agrees that City shall have access to any and all such Documents at any and all times, as deemed necessary by City, during said Retention Period. City may, at its election, require Vendor to return the documents to City at Vendor's expense prior to or at the conclusion of the Retention Period. In such event, Vendor may retain a copy of the documents.

Vendor shall notify City, immediately, in the event Vendor receives any requests for information from a third party, which pertain to the Documents referenced herein. Vendor understands and agrees that City will process and handle all such requests.

S.B. 943 – Disclosure Requirements for Certain Government Contracts. For contracts (1) with a stated expenditure of at least $1 million in public funds for the purchase of goods or services by the City, or (2) that result in the expenditure of at least $1 million in public funds for the purchase of goods or services by the City in a given fiscal year, Vendor acknowledges that the requirements of the Texas Public Information Act, Government Code, Chapter 552, Subchapter J, pertaining to the preservation and disclosure of Contracting Information maintained by the City or sent between the City and a vendor, contractor, potential vendor, or potential contractor, may apply to this bid and any resulting contract. Vendor agrees that the contract can be terminated if Vendor knowingly or intentionally fails to comply with a requirement of that subchapter.

By submitting a bid, Bidder warrants and certifies, and a contract awarded pursuant to this RFCSP is made in reliance thereon, that it, has not knowingly or intentionally failed to comply with this subchapter in a previous bid or contract. City hereby relies on Vendor's certification, and if found to be false, City may reject the bid or terminate the Contract for material breach.

Severability. If any clause or provision of this contract is held invalid, illegal or unenforceable under present or future federal, state or local laws, including but not limited to the City Charter, City Code, or ordinances of the City of San Antonio, Texas, then and in that event it is the intention of the parties hereto that such invalidity, illegality or unenforceability shall not affect any other clause or provision hereof and that the remainder of this contract shall be construed as if such invalid, illegal or unenforceable clause or provision was never contained herein. It is also the intention of the parties hereto that in lieu of each clause or provision of this contract that is invalid, illegal, or unenforceable, there be added as a part of the contract a clause or provision as similar in terms to such invalid, illegal or unenforceable clause or provision as may be possible, legal, valid and enforceable.

Compliance with Law. Vendor shall provide and perform all services required under this Agreement in compliance with all applicable federal, state and local laws, rules and regulations.

Certifications. Vendor warrants and certifies that Vendor and any other person designated to provide services hereunder has the requisite training, license and/or certification to provide said services, and meets all competence standards promulgated by all other authoritative bodies, as applicable to the services provided herein.

Non-waiver of Performance. Unless otherwise specifically provided for in this Agreement, a waiver by either Party of a breach of any of the terms, conditions, covenants or guarantees of this Agreement shall not be construed or held to be a waiver of any succeeding or preceding breach of the same or any other term, condition, covenant or guarantee herein contained. Further, any failure of either Party to insist in any one or more cases upon the strict performance of any of the covenants of this Agreement, or to exercise any option herein contained, shall in no event be construed as a waiver or relinquishment for the future of such covenant or option. In fact, no waiver, change, modification or discharge by either party hereto of any provision of this Agreement shall be deemed to have been made or shall be effective unless expressed in writing and signed by the party to be charged. No act or omission by a Party shall in any manner impair or prejudice any right, power, privilege, or remedy available to that Party hereunder or by law or in equity, such rights, powers, privileges, or remedies to be always specifically preserved hereby.

Venue. Venue of any court action brought directly or indirectly by reason of this contract shall be in Bexar County, Texas. This contract is made and is to be performed in Bexar County, Texas, and is governed by the laws of the State of Texas.

Non-discrimination. As a condition of entering into this agreement, Vendor represents and warrants that it will comply with the City's Commercial Nondiscrimination Policy, as described under Section III.C.1 of the SBEDA Ordinance. As part of such compliance, Vendor shall not discriminate on the basis of race, color, religion, ancestry or national origin, sex, age, marital status, sexual orientation, or on the basis of disability or other unlawful forms of discrimination in the solicitation, selection, hiring or commercial treatment of subcontractors, vendors, suppliers, or commercial customers, nor shall Vendor retaliate against any person for reporting instances of such discrimination. Vendor shall provide equal opportunity for subcontractors, vendors and suppliers to participate in all of its public sector and private sector subcontracting and supply opportunities, provided that nothing contained in this clause shall prohibit or limit otherwise lawful efforts to remedy the effects of marketplace discrimination that have occurred or are occurring in the City's Relevant Marketplace. Vendor understands and agrees that a material violation of this clause shall be considered a material breach of this agreement and may result in termination of this agreement, disqualification of Vendor from participating in City contracts, or other sanctions. This clause is not enforceable by or for the benefit of, and creates no obligation to, any third party. Vendor shall include this nondiscrimination clause in all subcontracts for the performance of this contract.

As a party to this contract, Vendor understands and agrees to comply with the *Non-Discrimination Policy* of the City of San Antonio contained in Chapter 2, Article X of the City Code and further, shall not discriminate on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, veteran status, age or disability, unless exempted by state or federal law, or as otherwise established herein.

Attorney's Fees. The Parties hereto expressly agree that, in the event of litigation, each party hereby waives its right to payment of attorneys' fees.

State Prohibitions on Contracts:

This section only applies to a contract that:

(1) is between a governmental entity and a company with 10 or more full-time employees; and
(2) has a value of $100,000 or more that is to be paid wholly or partly from public funds of the governmental entity.

"Company" means a for-profit organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including a wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate of those entities or business associations that exists to make a profit. This term does not include a sole proprietorship.

Prohibition on Contracts with Companies Boycotting Israel.

Texas Government Code §2271.002 provides that a governmental entity may not enter into a contract with a company for goods or services, unless the contract contains a written verification from the company that it: (1) does not boycott Israel; and (2) will not boycott Israel during the term of the contract.

"Boycott Israel" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes.

By submitting an offer to or executing contract documents with the City of San Antonio, Company hereby verifies that it does not boycott Israel, and will not boycott Israel during the term of the contract. City hereby relies on Company's verification. If found to be false, City may terminate the contract for material breach.

Prohibition on Contracts with Companies Boycotting Certain Energy Companies.

Texas Government Code §2274 provides that a governmental entity may not enter into a contract with a company for goods or services, unless the contract contains a written verification from the company that it: (1) does not boycott energy companies; and (2) will not boycott energy companies during the term of the contract.

"Boycott energy company" means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company: (A) engages in the exploration, production, utilization, transportation, sale, or manufacturing of fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; or (B) does business with a company described in (A).

By submitting an offer to or executing contract documents with the City of San Antonio, Company hereby verifies that it does not boycott energy companies and will not boycott energy companies during the term of the contract. City hereby relies on Company's verification. If found to be false, City may terminate the contract for material breach.

Prohibition on Contracts with Companies that Discriminate Against Firearm and Ammunition Industries.

Texas Government Code §2274 provides that a governmental entity may not enter into a contract with a company for goods or services, unless the contract contains a written verification from the company 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.

"Discriminate against a firearm entity or firearm trade association": (A) means, with respect to the entity or association, to: (i) refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (ii) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (iii) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association.

By submitting an offer to or executing contract documents with the City of San Antonio, Company hereby verifies that it does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association; and will not discriminate during the term of the contract against a firearm entity or firearm trade association. City hereby relies on Company's verification. If found to be false, City may terminate the contract for material breach.

Contracts with Companies Engaged in Business with Iran, Sudan, or Foreign Terrorist Organization Prohibited. Texas Government Code §2252.152 provides that a governmental entity may not enter into a governmental contract with a company that is identified on a list prepared and maintained under Texas Government Code §§2270.0201 or 2252.153. Vendor hereby certifies that it is not identified on such a list and that it will notify City should it be placed on such a list while under contract with City. City hereby relies on Vendor's certification. If found to be false, or if Vendor is identified on such list during the course of its contract with City, City may terminate the Contract for material breach.

Delinquent Taxes. In the event that Vendor is or subsequently becomes delinquent in the payment of taxes owed to the City of San Antonio, the City reserves the right to deduct any delinquent taxes from payments that the City may owe to the delinquent Vendor as a result of this contract.

Binding Contract. This contract shall be binding on and inure to the benefit of the parties hereto and their respective heirs, executors, administrators, legal representatives, and successors and assigns, except as otherwise expressly provided for herein.

Entire Agreement. This contract, including City's final electronically posted online version together with its authorizing ordinance and its price schedule(s), addendums, attachments, purchase orders, and exhibits, if any, and Respondent's proposal, constitutes the final and entire agreement between the parties hereto and contains all of the terms and conditions agreed upon. City's solicitation documents shall control over Respondent's proposal in the event of a conflict. No other agreements, oral or otherwise, regarding the subject matter of this contract shall be deemed to exist or to bind the parties hereto, unless same be in writing, dated subsequent to the date hereof, and be duly executed by the parties, in accordance with the Change Order provision herein. **Parties agree that City's final electronically posted online version of this**

solicitation contains the agreed upon specifications, scope of services, and terms and conditions of this contract, and shall control in the event of a conflict with any printed version signed and submitted by Vendor. Any addendums issued to the final electronically posted online version of this solicitation shall control in the event of a conflict therewith. Addendums shall be interpreted in order of the date issued, with those issued most recently taking priority.

007 - SIGNATURE PAGE

By submitting a proposal, Respondent represents that:

(s)he is authorized to bind Respondent to fully comply with the terms and conditions of City's Request for Competitive Sealed Proposals for the prices stated therein;

(s)he has read the entire document, including the final version issued by City, and agreed to the terms therein;

Respondent is in good standing with the Texas State Comptroller's Office; and

to the best of his/her knowledge, all information is true and correct.

Complete the following and sign on the signature line below. Failure to sign and submit this Signature Page will result in rejection of your proposal.

Respondent Information
Please Print or Type

Vendor ID No. _____

Signer's Name _____

Name of Business _____

Street Address _____

City, State, Zip Code _____

Email Address _____

Telephone No. _____

Fax No. _____

City's Solicitation No. _____

_____
Signature of Person Authorized to Sign Proposal

008 - STANDARD DEFINITIONS

Whenever a term defined by the Uniform Commercial Code ("UCC"), as enacted by the State of Texas, is used in the Contract, the UCC definition shall control, unless otherwise defined in the Contract.

All-or-None Proposal – a request for competitive sealed proposal in which the City will award the entire contract to one respondent only.

Alternate Proposal - two or more proposals with substantive variations in the item or service offered from the same respondent in response to a solicitation.

Assignment - a transfer of claims, rights or interests in goods, services or property.

Change Order - a change to the plans or specifications of the contract, or an increase or decrease in the quantity of work to be performed or of materials, equipment, or supplies to be furnished, issued by the Director after the proposal has been accepted by the City.

City - the City of San Antonio, a Texas home-rule municipal corporation.

Contract - the binding legal agreement between the City and Vendor.

Respondent - the respondent whose proposal is accepted by the City and is, therefore, the person, firm or entity providing goods or services to the City under a contract.

Director – the Director of City's Finance Department, or Director's designee.

Equal or Equivalent - terms to indicate that similar products or other brands may be acceptable for purchase if specifications and functional requirements are met.

Line Item - a listing of items in a proposal for which a respondent is expected to provide separate pricing.

Non-Responsive Proposal - a proposal or offer that does not comply with the terms and conditions, or specifications and/or requirements of the RFCSP.

Offer - a complete, signed response to an RFCSP that, if accepted, would bind Respondent to perform the resultant contract. The term "offer" is synonymous with the terms "bid" and "proposal".

Payment Bond - a particular form of security provided by the Respondent to protect the City against loss due to the Respondent's failure to pay suppliers and subcontractors.

Performance Bond - a particular form of security provided by the Respondent to protect the City against loss due to the Respondent's inability or unwillingness to complete the contract as agreed.

Performance Deposit - security provided by the Respondent to protect City against loss due to the Respondent's inability or unwillingness to complete the contract as agreed.

Pre-Submittal Conference - a meeting conducted by the City, held in order to allow respondents to ask questions about the proposed contract and particularly, the contract specifications.

Proposal - a complete, signed response to a solicitation. The term "proposal" is synonymous with the terms "offer" and "bid".

Proposal Bond or Proposal Guarantee - security to ensure that Respondent (a) will not withdraw the proposal within the period specified for acceptance, and (b) will furnish any required bonds or performance guarantees, and any necessary insurance within the time specified in the solicitation.

Proposal Opening - a public meeting during which proposal responses are opened and the names of respondents are read aloud.

Purchase Order - a validly issued order placed by an authorized City department for the purchase of goods or services, written on the City's standard purchase order form, and which is Vendor's authority to deliver to and invoice the City for the goods or services specified in a RFCSP for the price stated in Vendor's proposal.

Request for Competitive sealed Proposal (RFCSP) – a solicitation for a specified good or a service, evaluated on the basis of price and other factors.

Respondent - a person, firm or entity that submits a proposal in response to a solicitation. The respondent whose proposal is accepted by City may also be referred to herein as Respondent, Vendor or Supplier. The term "respondent" is synonymous with the term "bidder".

Responsible Offeror - a respondent who is known to have the necessary competence and qualifications to perform and provide all requirements of an intended contract.

Responsive Offeror - a respondent who tenders a proposal which meets all requirements of the RFCSP and is a responsible offeror.

Sealed Proposal - a proposal submitted as a sealed document by a prescribed time to the location indicated in the RFCSP. The contents of the proposal will not be made public prior to the award of the contract.

Specifications - a description of what the City requires and what the respondent must offer; a description of the physical or functional characteristics of a product or material, or the nature of a service or construction item.

Subcontractor - a person, firm or entity providing goods or services to a vendor to be used in the performance of the Vendor's obligations under the contract with City.

Supplier - the respondent whose proposal is accepted by the City and is, therefore, the person, firm or entity providing goods or services to the City under a contract.

Vendor - the respondent whose proposal is accepted by the City and is, therefore, the person, firm or entity providing goods or services to the City under a contract.

Waiver of Irregularity – noting but disregarding an immaterial variance within a proposal.

009 - ATTACHMENTS

RFCSP ATTACHMENT A, PART ONE

GENERAL INFORMATION

1. Respondent Information: Provide the following information regarding the Respondent.
(NOTE: Co-Respondents are two or more entities proposing as a team or joint venture with each signing the contract, if awarded. Sub-contractors are not Co-Respondents and should not be identified here. If this proposal includes Co-Respondents, provide the required information in this Item #1 for each Co-Respondent by copying and inserting an additional block(s) before Item #2.)

Respondent Name: _____
(NOTE: Give exact legal name as it will appear on the contract, if awarded.)

Principal Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No:_____

Website address:_____

Year established: _____

Provide the number of years in business under present name: _____

Social Security Number or Federal Employer Identification Number: _____

Texas Comptroller's Taxpayer Number, if applicable: _____
(NOTE: This 11-digit number is sometimes referred to as the Comptroller's TIN or TID.)

DUNS NUMBER: _____

Business Structure: Check the box that indicates the business structure of the Respondent.

___Individual or Sole Proprietorship If checked, list Assumed Name, if any: _____
___ Partnership
___Corporation If checked, check one: ___For-Profit ___ Nonprofit
Also, check one: ___Domestic ___Foreign
___Other If checked, list business structure: _____

Printed Name of Contract Signatory: _____
Job Title: _____

Provide any other names under which Respondent has operated within the last 10 years and length of time under for each:

_____
_____
_____

Provide address of office from which this project would be managed:
City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Annual Revenue: $_____

Total Number of Employees: _____

Total Number of Current Clients/Customers: _____

Briefly describe other lines of business that the company is directly or indirectly affiliated with:

_____
_____
_____

List Related Companies:

_____
_____
_____

2. **Contact Information:** List the one person who the City may contact concerning your proposal or setting dates for meetings.

Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Email: _____

3. Does Respondent anticipate any mergers, transfer of organization ownership, management reorganization, or departure of key personnel within the next twelve (12) months?

Yes ___ No ___

4. Is Respondent authorized to do business in the State of Texas?

Yes ___ No ___ If "Yes", provide Texas Secretary of State registration number..

_____

_____

5. Where is the Respondent's corporate headquarters located? _____

6. **Local/County Operation**: Does the Respondent have an office located in San Antonio, Texas?

Yes ___ No ___ If "Yes", respond to a and b below:

a. How long has the Respondent conducted business from its San Antonio office?

Years _____ Months_____

b. State the number of full-time employees at the San Antonio office.

If "No", indicate if Respondent has an office located within Bexar County, Texas:

Yes ___ No ___ If "Yes", respond to c and d below:

c. How long has the Respondent conducted business from its Bexar County office?

Years _____ Months_____

d. State the number of full-time employees at the Bexar County office. _____

7. **Debarment/Suspension Information**: Has the Respondent or any of its principals been debarred or suspended from contracting with any public entity?

Yes ___ No ___ If "Yes", identify the public entity and the name and current phone number of a representative of the public entity familiar with the debarment or suspension, and state the reason for or circumstances surrounding the debarment or suspension, including but not limited to the period of time for such debarment or suspension.

_____
_____

8. **Surety Information**: Has the Respondent ever had a bond or surety canceled or forfeited?

   Yes ___ No ___ If "Yes", state the name of the bonding company, date, amount of bond and reason for such cancellation or forfeiture.

   _____
   _____

9. **Bankruptcy Information**: Has the Respondent ever been declared bankrupt or filed for protection from creditors under state or federal proceedings?

   Yes ___ No ___ If "Yes", state the date, court, jurisdiction, cause number, amount of liabilities and amount of assets.

   _____
   _____

10. **Disciplinary Action:** Has the Respondent ever received any disciplinary action, or any pending disciplinary action, from any regulatory bodies or professional organizations? If "Yes", state the name of the regulatory body or professional organization, date and reason for disciplinary or impending disciplinary action.

    _____
    _____

11. **Previous Contracts:**

    a. Has the Respondent ever failed to complete any contract awarded?

       Yes ___ No ___ If "Yes", state the name of the organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

       _____
       _____

    b. Has any officer or partner proposed for this assignment ever been an officer or partner of some other organization that failed to complete a contract?
       Yes ___ No ___ If "Yes", state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

       _____
       _____

    c. Has any officer or partner proposed for this assignment ever failed to complete a contract handled in his or her own name?

       Yes ___ No ___ If "Yes", state the name of the individual, organization contracted with, services contracted, date, contract amount and reason for failing to complete the contract.

       _____
       _____

12. **Financial Review:** Is your firm publicly traded? Yes ___ No ___ If "Yes", provide your firm's SEC filing number.

    _____

REFERENCES

Provide three (3) reference letters from three (3) separate organizations/companies/firms, that the Respondent has provided services to within the past three (3) years.

The contact person named on the reference letter should be familiar with the day-to-day management of the contract and would be able to provide type, level, and quality of services performed. In addition, please provide the contact information below of the references you have submitted.

Reference No. 1:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Email: _____

Date and Type of Service(s) Provided: _____

_____

Reference No. 2:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Email: _____

Date and Type of Service(s) Provided: _____

_____

Reference No. 3:

Firm/Company Name _____

Contact Name: _____ Title: _____

Address: _____

City: _____State: _____Zip Code: _____

Telephone No._____ Fax No: _____

Email: _____

Date and Type of Service(s) Provided: _____

_____

RFCSP ATTACHMENT A, PART TWO

EXPERIENCE, BACKGROUND, QUALIFICATIONS

Prepare and submit narrative responses to address the following items. If Respondent is proposing as a team or joint venture, provide the same information for each member of the team or joint venture. Provide response below each item.

1. Describe Respondent's experience relevant to the Scope of Services requested by this RFCSP. List and describe relevant projects of similar size and scope performed over the past four years. Identify associated results or impacts of the project/work performed.

2. Describe Respondent's specific experience with public entities clients, especially large municipalities. If Respondent has provided services for the City in the past, identify the name of the project and the department for which Respondent provided those services.

3. List other resources, including total number of employees, number and location of offices, number and types of equipment available to support this project.

4. If Respondent is proposing as a team or joint venture or has included sub-contractors, describe the rationale for selecting the team and the extent to which the team, joint ventures and/or sub-contractors have worked together in the past.

5. Identify the number and professional qualifications (to include licenses, certifications, associations) of staff to be assigned to the project and relevant experience on projects of similar size and scope.

6. State the primary work assignment and the percentage of time key personnel will devote to the project if awarded the contract.

7. Additional Information. Identify any additional skills, experiences, qualifications, and/or other relevant information about the Respondent's qualifications.

RFCSP ATTACHMENT A, PART THREE

PROPOSED PLAN

Prepare and submit the following items. Provide response below each item.

1. Operating Plan – Describe the proposed plan to conduct operations, including service categories, specific tasks, staff assigned and schedule of events.

2. Maintenance Plan – Describe Plan to ensure maintenance of facility throughout term of the contract. Identify proposed tasks and schedule.

3. Reporting – Describe overall reporting approach for the new solution. Reports are defined as any document produced out of the new solution. This may include, but not limited to: Standardized and parameterized reports, Ad-hoc query and reporting.

4. Test Strategy – Describe overall approach and ability to test and validate the functionality of the implemented solution against the documented requirements. This section should include:
   i. Unit Testing
   ii. System Testing
   iii. Performance and Reliability Testing
   iv. Functional and User Acceptance Testing
   v. Regression Testing
   vi. Data Conversion Testing
   vii. Test Plans
   viii. Test Scripts
   ix. Issue Management and Resolution

5. Service Level Agreement –
   i. Service Availability - 99.9%: system can be down for less than 10 minutes per week factoring a 24/7 schedule.
   ii. System Recovery Time Objective (RTO) - 4 hours: the maximum time system can be offline before services are restored to end users
   iii. System Recovery Point Objective (RPO) - 24 Hours: represents the frequency in which we are capturing snapshots of data in an offsite or backup location – in the event the primary site goes offline

6. Additional Information: Provide any additional plans and/or relevant information about Respondent's approach to providing the required services

RFCSP ATTACHMENT B

PRICE SCHEDULE

Indicate a fixed price per line item / sub-line item for performing the services as specified in this RFCSP. **Respondent must propose fixed price for each item / sub-line item of the Price Schedule or Respondent's proposal may be deemed non-responsive**.

Respondent's proposal must be based on the proposed contract term, including renewal periods, stated in this RFCSP. Proposing a different term of contract, or renewal terms may lead to disqualification of Respondent's proposal from consideration. As such, Respondent must provide pricing in the manner set forth in the RFCSP's Price Schedule. Failure to do so may lead to disqualification of respondent's proposal from consideration.

Bidder will be deemed non-responsive for line items submitted by Bidder as: "No Bid" or "left blank". Line items marked by Bidder as "Included", "N/C", or $0.00 will be determined by the City as Bidder will provide service to City at No Charge.

(Posted as a separate document)

RFCSP ATTACHMENT C

LITIGATION DISCLOSURE FORM

Respond to each of the questions below by checking the appropriate box. Failure to fully and truthfully disclose the information required by this Litigation Disclosure form may result in the disqualification of your proposal from consideration or termination of the contract, once awarded.

Have you or any member of your Firm or Team to be assigned to this engagement ever been indicted or convicted of a felony or misdemeanor greater than a Class C in the last five (5) years?

Yes ___ No ___

Have you or any member of your Firm or Team to be assigned to this engagement been terminated (for cause or otherwise) from any work being performed for the City of San Antonio or any other Federal, State or Local Government, or Private Entity?

Yes ___ No ___

Have you or any member of your Firm or Team to be assigned to this engagement been involved in any claim or litigation with the City of San Antonio or any other Federal, State or Local Government, or Private Entity during the last ten (10) years?

Yes ___ No ___

If you have answered "Yes" to any of the above questions, please indicate the name(s) of the person(s), the nature, and the status and/or outcome of the information, indictment, conviction, termination, claim or litigation, as applicable. Any such information should be provided on a separate page, attached to this form and submitted with your proposal.

RFCSP ATTACHMENT D

VETERAN-OWNED SMALL BUSINESS (VOSB) PREFERENCE PROGRAM TRACKING FORM

(Posted as a separate document)

RFCSP ATTACHMENT E

MANDATORY FEDERAL PROVISIONS

(Posted as a separate document)

RFCSP ATTACHMENT F

COSA ACCEPTABLE USE OF INFORMATION TECHNOLOGY

(Posted as a separate document)

RFCSP ATTACHMENT G

THIRD PARTY VENDOR IT CLOUD SECURITY QUESTIONNAIRE

(Posted as a separate document)

RFCSP ATTACHMENT H

COSA ACCESS CONTROL

(Posted as a separate document)

RFCSP ATTACHMENT I

COSA DATA SECURITY

(Posted as a separate document)

RFCSP ATTACHMENT J

PRE-SUBMITTAL CONFERENCE AGENDA

(Posted as a separate document)

RFCSP ATTACHMENT K

PROPOSAL CHECKLIST REVISION I

Respondent shall limit any reference to the Respondent's proposed price to the respective section designated for this information. PLACING PRICE INFORMATION IN OTHER SECTIONS OF A RESPONSE TO THIS RFCSP MAY RESULT IN THE RESPONDENT'S PROPOSAL BEING DEEMED NON-RESPONSIVE AND THEREFORE DISQUALIFIED FROM CONSIDERATION.

Use this checklist to ensure that all required documents have been included in the proposal and appear in the correct order.

Document	Initial to Indicate Document is Attached to Proposal
Table of Contents	
Executive Summary	
General Information and Three (3) Reference Letters RFCSP Attachment A Part One	
Experience, Background & Qualifications RFCSP Attachment A Part Two	
Proposed Plan RFCSP Attachment A Part Three	
Price Schedule RFCSP Attachment B	
+Contracts Disclosure form	
Litigation Disclosure Form RFCSP Attachment C	
+Veteran-Owned Small Business Program Tracking Form RFCSP Attachment D	
+Certificate of Interested Parties (Form 1295)	
Proof of Insurability Insurance Provider's Letter AND Copy of Current Certificate of Insurance	
Financial Information	
Third Party Vendor IT Cloud Security Questionnaire RFCSP Attachment G	
+Signature Page RFCSP Section 007	
Proposal Checklist RFCSP Attachment K	
+ Addendum, if any	
One **COMPLETE** electronic copy	

+ Documents marked with a "+" on this checklist require a signature.

Be sure all forms that require a signature are done so prior to submittal of proposal.

RFCSP ATTACHMENT L

PRE-SUBMITTAL CONFERENCE SIGN-IN SHEET

(Posted as a separate document)

RFCSP ATTACHMENT B - PRICE SCHEDULE

RFCSP 22-079, 6100015294, Rideshare Monitoring Services for San Antonio International Airport

Respondent Name:			
Provide the following information regarding Respondent's software and submit with your proposal the appropriate Attachments G if a SaaS solution is proposed.			
Software is Off-Premise Vendor Hosted:	☐ Yes	or	☐ No
Software is On-Premise City Hosted:	☐ Yes	or	☐ No

Item	Initial Period	Year 2	3	4	5	Total Cost
1. What is the TOTAL, all-inclusive - System Application - cost for ALL software being proposed in the proposed system?						
1A System Application						
One-time License Fee with 1 Year Warranty						0
Recurring license fee						0
Annual Maintenance Fee						0
One-Time Setup Fee						0
Hosting / Service Cost						0
1B Other Software - One-time License Fee						
Database						0
Software						0
Operating System and Utilities						0
Development Tools						0
Reporting Tools						0
Other Software - One Time Fee						0
1C Other Software - Re-Occurring Maintenance/Support Fee						
Database						0
Software						0
Operating System and Utilities						0
Development Tools						0
Reporting Tools						0
Other Software - One Time Fee						0
2. What is the TOTAL, all-inclusive - Specialized Hardware - cost for ALL software being proposed in the proposed system?						
2A Specialized Hardware - One Time Cost						
(vendor to provide list and costs)						0
						0
						0
						0
2B Specialized Hardware - Re-Occurring Maintenance/Support						
(vendor to provide list and costs)						0
						0
						0

RFCSP ATTACHMENT B - PRICE SCHEDULE

RFCSP 22-079, 6100015294, Rideshare Monitoring Services for San Antonio International Airport

3. What is the TOTAL, all-inclusive - Solution Implementation cost for ALL software being proposed in the proposed system?						
3a. Project Initiation and Management						0
3b. Functional Requirements/Validation						0
3c. Software Installation						0
3d. System Design						0
3e. System Configuration						0
3f. Development- Customization						0
3g. Development-Integration						0
3h. Development - Other						0
3i. Conversion/Migration						0
3j. System Testing						0
3k. Training Deployment						0
3l. Cut-Over, Go-Live, Post Go Live						0
3m. Final Acceptance Testing						0
3n. Other-Implementation						0
4. What is the TOTAL, all-inclusive - Other Costs for ALL software being proposed in the proposed system?						
(vendor to provide list and costs)						
						0
						0
Total Fixed Cost	0					0
Total Recurring Costs		0	0	0	0	0
Total system cost						**0**

City of San Antonio

Veteran-Owned Small Business Program Tracking Form

Authority. San Antonio City Code Chapter 2, Article XI describes the City's veteran-owned small business preference program.

Tracking. **This solicitation is not eligible for a preference** based on status as a veteran-owned small business (VOSB). Nevertheless, in order to determine whether the program can be expanded at a later date, the City tracks VOSB participation at both prime contract and subcontract levels.

Certification. The City relies on inclusion in the database of veteran-owned small businesses (VOSB) maintained by the U.S. Small Business Administration to verify VOSB status; however, veteran status may also be confirmed by certification by another public or private entity that uses similar certification procedures.

Definitions.

The program uses the federal definitions of veteran and veteran-owned small business found in 38 CFR Part 74.

- The term "veteran" means a person who served on active duty with the U.S. Army, Air Force, Navy, Marine Corps, Coast Guard, for any length of time and at any place and who was discharged or released under conditions other than dishonorable. Reservists or members of the National Guard called to federal active duty or disabled from a disease or injury incurred or aggravated in line of duty or while in training status.

- A veteran-owned small business is a business that is not less than 51 percent owned by one or more veterans, or in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; the management and daily business operations of which are controlled by one or more veterans and qualifies as "small" for Federal business size stand purposes.

The program uses the below definition of joint venture.

- Joint Venture means a collaboration of for-profit business entities, in response to a solicitation, which is manifested by a written agreement, between two or more independently owned and controlled business firms to form a third business entity solely for purposes of undertaking distinct roles and responsibilities in the completion of a given contract. Under this business arrangement, each joint venture partner shares in the management of the joint venture and also shares in the profits or losses of the joint venture enterprise commensurately with its contribution to the venture.

The program does not distinguish between a veteran and a service-disabled veteran-owned business and is not limited geographically.

COMPLETE THE FOLLOWING FORM AND SUBMIT WITH YOUR BID/PROPOSAL.

INSTRUCTIONS

- IF SUBMITTING AS A PRIME CONTRACTOR ONLY, COMPLETE **SECTION 1** OF THIS FORM.

- IF SUBMITTING AS A PRIME CONTRACTOR UTILIZING A SUBCONTRACTOR, COMPLETE **SECTIONS 1 AND 2** OF THIS FORM.

City of San Antonio

Veteran-Owned Small Business Program Tracking Form

SOLICITATION NAME/NUMBER: _____

Name of Respondent:		
Physical Address:		
City, State, Zip Code:		
Phone Number:		
Email Address:		
Is Respondent certified as a VOSB with the U.S. Small Business Administration? (circle one)	Yes	No
If yes, provide the SBA Certification #		
If not certified by the SBA, is Respondent certified as a VOSB by another public or private entity that uses similar certification procedures? (circle one)	Yes	No
If yes, provide the name of the entity who has certified Respondent as a VOSB. Include any identifying certification numbers.		
Participation Percentage:		
Participation Dollar Amount:		

Is Respondent subcontracting with a business that is certified as a VOSB? (circle one)	Yes	No
Name of **SUBCONTRACTOR** Veteran-Owned Small Business:		
Physical Address:		
City, State, Zip Code:		
Phone Number:		
Email Address:		
Is **SUBCONTRACTOR** certified as a VOSB with the U.S. Small Business Administration? (circle one)	Yes	No
If yes, provide the SBA Certification #		
If not certified by the SBA, is **SUBCONTRACTOR** certified as a VOSB by another public or private entity that uses similar certification procedures? (circle one)	Yes	No
If yes, provide the name of the entity who has certified **SUBCONTRACTOR** as a VOSB. Include any identifying certification numbers.		
Participation Percentage:		
Participation Dollar Amount		

ACKNOWLEDGEMENT

THE STATE OF TEXAS

I certify that my responses and the information provided on this Veteran-Owned Small Business Preference Program Identification Form are true and correct to the best of my personal knowledge and belief and that I have made no willful misrepresentations on this form, nor have I withheld any relevant information in my statements and answers to questions. I am aware that any information given by me on this Veteran-Owned Small Business Preference Program Identification Form may be investigated and I hereby give my full permission for any such investigation, including the inspection of business records and site visits by City or its authorized representative. I fully acknowledge that any misrepresentations or omissions in my responses and information may cause my offer to be rejected or contract to be terminated. I further acknowledge that providing false information is grounds for debarment.

BIDDER/RESPONDENT'S FULL NAME:

_____

(Print Name) Authorized Representative of Bidder/Respondent

_____

(Signature) Authorized Representative of Bidder/Respondent

_____

Title

_____

Date

This Veteran-Owned Small Business Program Tracking Form must be submitted with the Bidder/Respondent's bid/proposal.

ATTACHMENT G

MANDATORY FEDERAL CONTRACT PROVISIONS

I. TITLE VI NOTICE

The City of San Antonio in accordance with the provisions of Title VI of the Civil Rights Act of 1964 (78 Stat. 252, 42 U.S.C. §§ 2000d to 2000d-4) and the Regulations, hereby notifies all bidders that it will affirmatively ensure that any contract entered into pursuant to this advertisement, disadvantaged business enterprises will be afforded full and fair opportunity to submit bids in response to this invitation and will not be discriminated against on the grounds of race, color, or national origin in consideration for an award.

II.GENERAL CIVIL RIGHTS PROVISIONS

The contractor agrees to comply with pertinent statutes, Executive Orders and such rules as are promulgated to ensure that no person shall, on the grounds of race, creed, color, national origin, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

This provision binds the contractor and subtier contractors from the bid solicitation period through the completion of the contract. This provision is in addition to that required of Title VI of the Civil Rights Act of 1964.

III. TITLE VI CLAUSES COMPLIANCE WITH NONDISCRIMINATION REQUIREMENTS

During the performance of this contract, the contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "contractor") agrees as follows:

1. **Compliance with Regulations:** The contractor (hereinafter includes consultants) will comply with the Title VI List of Pertinent Nondiscrimination Acts And Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.

2. **Non-discrimination:** The contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, or national origin in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The contractor will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21.

3. **Solicitations for Subcontracts, Including Procurements of Materials and Equipment:** In all solicitations, either by competitive bidding, or negotiation made by the contractor for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by the contractor of the contractor's obligations under this contract and the Nondiscrimination Acts And Authorities on the grounds of race, color, or national origin.

4. **Information and Reports:** The contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the sponsor or the Federal Aviation Administration to be pertinent to ascertain compliance with such Nondiscrimination Acts And Authorities and instructions. Where any information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, the contractor will so certify to the sponsor or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

5. **Sanctions for Noncompliance:** In the event of a contractor's noncompliance with the Non-discrimination provisions of this contract, the sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

a. Withholding payments to the contractor under the contract until the contractor complies; and/or
b. Cancelling, terminating, or suspending a contract, in whole or in part.

6. **Incorporation of Provisions:** The contractor will include the provisions of paragraphs one through six in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations and directives issued pursuant thereto. The contractor will take action with respect to any subcontract or procurement as the sponsor or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the contractor may request the sponsor to enter into any litigation to protect the interests of the sponsor. In addition, the contractor may request the United States to enter into the litigation to protect the interests of the United States.

IV. TITLE VI LIST OF PERTINENT NONDISCRIMINATION ACTS AND AUTHORITIES

During the performance of this contract, the contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "contractor") agrees to comply with the following non-discrimination statutes and authorities; including but not limited to:

- Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d *et seq*., 78 stat. 252), (prohibits discrimination on the basis of race, color, national origin);
- 49 CFR part 21 (Non-discrimination In Federal
- ly-Assisted Programs of The Department of Transportation—Effectuation of Title VI of The Civil Rights Act of 1964);
- The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 U.S.C. § 4601), (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);
- Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794 *et seq*.), as amended, (prohibits discrimination on the basis of disability); and 49 CFR part 27;
- The Age Discrimination Act of 1975, as amended, (42 U.S.C. § 6101 *et seq*.), (prohibits discrimination on the basis of age);
- Airport and Airway Improvement Act of 1982, (49 USC § 471, Section 47123), as amended, (prohibits discrimination based on race, creed, color, national origin, or sex);
- The Civil Rights Restoration Act of 1987, (PL 100-209), (Broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, The Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);
- Titles II and III of the Americans with Disabilities Act of 1990, which prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131 – 12189) as implemented by Department of Transportation regulations at 49 CFR parts 37 and 38;
- The Federal Aviation Administration's Non-discrimination statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);
- Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures non-discrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;
- Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable

steps to ensure that LEP persons have meaningful access to your programs (70 Fed. Reg. at 74087 to 74100);

- Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 U.S.C. 1681 et seq).

V. FEDERAL FAIR LABOR STANDARDS ACT

All contracts and subcontracts that result from this solicitation incorporate by reference the provisions of 29 CFR part 201, the Federal Fair Labor Standards Act (FLSA), with the same force and effect as if given in full text. The FLSA sets minimum wage, overtime pay, recordkeeping, and child labor standards for full and part time workers.

The contractor has full responsibility to monitor compliance to the referenced statute or regulation. The contractor must address any claims or disputes that arise from this requirement directly with the U.S. Department of Labor – Wage and Hour Division.

VI. OCCUPATIONAL SAFETY AND HEALTH ACT OF 1970

All contracts and subcontracts that result from this solicitation incorporate by reference the requirements of 29 CFR Part 1910 with the same force and effect as if given in full text. Contractor must provide a work environment that is free from recognized hazards that may cause death or serious physical harm to the employee. The contractor retains full responsibility to monitor its compliance and their subcontractor's compliance with the applicable requirements of the Occupational Safety and Health Act of 1970 (20 CFR Part 1910). Contractor must address any claims or disputes that pertain to a referenced requirement directly with the U.S. Department of Labor – Occupational Safety and Health Administration.

VII. DRUG-FREE WORKPLACE

(a) Definitions. As used in this clause—

"Controlled substance" means a controlled substance in schedules I through V of section 202 of the Controlled Substances Act (21 U.S.C. 812) and as further defined in regulation at 21 CFR 1308.11 - 1308.15.

"Conviction" means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the Federal or State criminal drug statutes.

"Criminal drug statute" means a Federal or non-Federal criminal statute involving the manufacture, distribution, dispensing, possession, or use of any controlled substance.

"Drug-free workplace" means the site(s) for the performance of work done by the Contractor in connection with a specific contract where employees of the Contractor are prohibited from engaging in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance.

"Employee" means an employee of a Contractor directly engaged in the performance of work under a Government contract. "Directly engaged" is defined to include all direct cost employees and any other Contractor employee who has other than a minimal impact or involvement in contract performance.

"Individual" means an offeror/contractor that has no more than one employee including the offeror/contractor.

(b) The Contractor, if other than an individual, shall—within 30 days after award (unless a longer period is agreed to in writing for contracts of 30 days or more performance duration), or as soon as possible for contracts of less than 30 days performance duration—

(1) Publish a statement notifying its employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition;

(2) Establish an ongoing drug-free awareness program to inform such employees about—

(i) The dangers of drug abuse in the workplace;

(ii) The Contractor's policy of maintaining a drug-free workplace;

(iii) Any available drug counseling, rehabilitation, and employee assistance programs; and
(iv) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(3) Provide all employees engaged in performance of the contract with a copy of the statement required by paragraph (b) (1) of this clause;

(4) Notify such employees in writing in the statement required by paragraph (b) (1) of this clause that, as a condition of continued employment on this contract, the employee will—
(i) Abide by the terms of the statement; and
(ii) Notify the employer in writing of the employee's conviction under a criminal drug statute for a violation occurring in the workplace no later than 5 days after such conviction;

(5) Notify the Contracting Officer in writing within 10 days after receiving notice under subdivision (b)(4)(ii) of this clause, from an employee or otherwise receiving actual notice of such conviction. The notice shall include the position title of the employee;

(6) Within 30 days after receiving notice under subdivision (b) (4) (ii) of this clause of a conviction, take one of the following actions with respect to any employee who is convicted of a drug abuse violation occurring in the workplace:
(i) Taking appropriate personnel action against such employee, up to and including termination; or
(ii) Require such employee to satisfactorily participate in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency; and

(7) Make a good faith effort to maintain a drug-free workplace through implementation of paragraphs (b) (1) through (b) (6) of this clause.

(c) The Contractor, if an individual, agrees by award of the contract or acceptance of a purchase order, not to engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance while performing this contract.

(d) In addition to other remedies available to the Government, the Contractor's failure to comply with the requirements of paragraph (b) or (c) of this clause may, pursuant to FAR 23.506, render the Contractor subject to suspension of contract payments, termination of the contract or default, and suspension or debarment.

CITY OF SAN ANTONIO

Administrative Directive	**7.4A Acceptable Use of Information Technology**
Procedural Guidelines	Regarding use of electronic communications systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Revisions Date(s)	December 14, 2017
Review Date	
Owner	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides guidance for the acceptable use of information technology systems including electronic devices, electronic mail, Internet access, and/or software among other City systems. This includes acceptable use of City-owned computers, mobile devices and/or personal. This directive establishes and identifies responsibility for the acceptable use of technology to help ensure the confidentiality, integrity and availability of City systems.

The City of San Antonio (COSA or City) provides access and use of its information technology systems to help users efficiently and effectively perform their business-related activities. All users of the City's information technology systems are responsible for using that technology in an appropriate and lawful manner.

Inappropriate use of information technology exposes the City to additional internal and/or external vulnerabilities that may reduce the reliability, confidentiality, integrity and/or availability of those systems.

The Information Technology Services Department (ITSD) shall be responsible for developing, maintaining, publishing and administering the acceptable use of information technology assets and systems. All unauthorized access to City data is strictly prohibited.

The City's information technology systems are shared resources that serve all of its users and provide the general public with access to its website. Inappropriate use of information system assets reduces the usefulness of these resources.

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Definitions	
Bring Your Own Device (BYOD)	The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.
City-administered information technology systems	Any technology or equipment that is used and/or managed by the City even if the City does not own the technology or equipment. City-managed information technology systems include technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Information Technology systems includes but, are not limited to computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and email messages, among other physical and virtual infrastructure.
Digital Signature	An electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.
Electronic mail	An electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with record the message.
Electronic Record	Record created, generated, sent, communicated, received, or stored by electronic means.
Electronic Signature	An electronic sound, symbol, or process attached to, or logically associated with a record and executed or adopted by a person with the intent to sign the record.
Generic Account	A generic account is any non-person account that may allow multiple users to use a single account to authenticate to the City network, application or other resource.
Incidental Use	Personal use of technology that does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology systems, and is not prohibited by this policy.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record
Malware	Malicious software designed to impact the confidentiality, integrity and/or availability of an information technology system. Malware can include viruses, worm, Trojan Horse, or adware among other malicious programs.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Records Management Officer	The person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record before it is eligible for destruction.

Software	**Authorized Software-** Authorized software is any program, code or installable executable file that has been tested and approved by ITSD. Authorized software constitutes any program, code or executable file deemed necessary to meet business needs. This includes Shareware, Freeware and Open Source software that meets the criteria stated in this policy. **Unauthorized Software-** Unauthorized software is any program, code or installable executable file that has not be tested and approved by ITSD or not necessary for business needs. This includes Shareware, Freeware, Open Source pirated software or copyright infringement in the use of software. For purposes of this policy, pirated software or copyright infringement includes illegally copied and/or downloaded software that violates licensing restrictions.
Sponsor	Departmental representative responsible for authorizing non-employee access to COSA assets and/or systems.
User	Any employee or non-employee who uses COSA-administered information assets and/or systems, exclusive of COSA's web pages

Policy

COSA is required to protect public assets and resources, and it has an obligation to manage information technology systems to comply with Chapter 552 of the Texas Public Information Act (open public records), Sections 7.71-7.79 of the Texas Administrative Code and 205.001-205.009 of the Local Government Code, among other regulations.

The National Institute of Standards of Technology (NIST) and industry best practices has been adopted by the City to help maintain the confidentiality, integrity and availability of COSA systems.

This directive pertains to all information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any other organization on behalf of the City.

- All information technology assets and systems, procured with City funds and/or used in the conduct of City business.
- All access to the City's facilities and networks, data, and/or applications among other systems including employees, contractors, vendors, and other third parties of City information assets, systems.
- All electronic messaging, equipment, or technology that is owned or administered by the City including City-owned computers, mobile devices, and/or personal devices is included within the scope of this Directive.
- All software, information systems and/or other documents developed by City personnel with City funds or licensed to the City of San Antonio.
- All data processed, stored, and/or transmitted by any City information technology system.
- All devices that use the COSA network, including any "Bring Your Own Device" (BYOD).

Adherence to this directive will help assure the City's acceptable use of technology.

- City-managed information technology systems shall be used for official business only, which may include personal communications, including telephone calls during business hours, that are necessary and in the interest of the City. While some incidental use (as defined below) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.
- There shall be no expectation of privacy when using any City-administered information

technology system including internet access for any information input or reviewed from City or personal accounts while in contact with City systems, social media, personal email accounts, SMS messages or instant messaging.

- All information generated, processed, stored, or entrusted on any City-provided information technology system is the property of COSA.
- COSA data shall be stored on network drives and not local drives. Local drives are not included in the City's backup strategy.
- Protected data per AD 7.3A Data Security (e.g. HIPAA, CJIS, Sensitive Personally Identifiable Information (PII) stored on laptop hard drives or removable media shall be authorized by the data owner and use ITSD approved encryption.
- Externally transmitted data by any technological means that contains protected data per AD 7.3A Data Security (e.g. HIPAA, CJIS, and Sensitive PII) shall use ITSD approved encryption.
- Business email received on COSA account shall not be manually or automatically forwarded or redirected to email addresses outside of COSA.
- A generic login account will only be allowed for specific business need. A written justification must be submitted to ITSD for approval. Generic network user account will not have email access.
- Email messages not essential to the fulfillment of statutory obligations or to the documentation of the City's functions may be deleted. Note: These messages may include personal messages, internal meeting notices, letters of transmittal, and general FYI announcements.
- Email messages that fulfill statutory obligations or document the City's functions are subject to retention as established by the Texas Administrative Code referenced in the Retention and Disposition of Email section.
- Individual COSA email accounts may not be used to send to more than 50 recipients of the same email message.
- Emails in deleted folder will be purged after 14 days.
- City distribution list shall not be made available for use by external email accounts.
- Distribution list must be maintained by owner to remove invalid email addresses.

Personal Use Policy

Personal use of technology must not interfere with the performance of assigned duties, must not have a detrimental effect on any City information technology system, and not be prohibited by this policy.

This includes the personal use of City-owned or managed technology that:

- Does not cause any additional expense to the City and is infrequent and brief
- Does not have a negative impact on overall user productivity
- Does not interfere with the normal operations of the user's department or work unit and does not compromise the City in anyway
- Does not embarrass either the City or the user
- Does not contravene other elements of this policy and serves the interest of the City in allowing employees to address personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that can be in the interest of the City include:

- Communications to alert household members about working late or other schedule changes
- Communications to make alternative child care arrangements, communications with doctors, hospital staff or day care providers
- Communications to determine the safety of family or household members, particularly in an emergency communications to reach businesses or governmental agencies that only can be

contacted during work hours and communications to arrange emergency repairs to vehicles or residences.

Security and Proprietary Information

Information stored on any City-administered information technology system should be classified in accordance with federal, state and local statues, ordinances, regulations, and/or policies among other directives regarding the confidentiality of the information (AD 7.3a Data Security). Users must comply with all City Directives regarding use of information technology, including:

- Electronic Communications (e-mail, voice and Internet)
- Password Management
- Security
- Data Management and Classification Monitoring
- Remote Access

All personal computers, laptops, and workstations should be protected from unauthorized access when the system is unattended. The recommended method of security for City devices is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for most Microsoft Operating Systems). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.

1. All BYOD devices used for work related tasks must be in compliance with AD 7.10 Mobile Device Security in order to obtain COSA email access; remote access etc. and the owner of the device must install and maintain security related software (operating system updates, Anti-virus/malware protection, etc.). ITSD has the right to refuse the use of any personal device for COSA related use if the device cannot be secured based on the standards and policies stated in this document. It is the responsibility of the owner to report if the device is lost or stolen immediately to ITSD.
2. User must take reasonable and necessary precautions to secure and protect electronic devices.
3. ITSD regularly maintains operating systems, updates security software, and applies security patches by sending those updates during non-business hours to computers attached to the network. When a user leaves for the day, he/she must log off from his/her computer, but leave the computer turned on and attached to the network. Laptops must be connected to the network at least once a month for at least 24 hours in order to receive updates.
4. As a regular maintenance step, at least once a week, save and close open files and applications then power off computer completely. Once the computer has powered down, power it back on. As computers are used on a daily basis, applications, files opened and web browsing slowly consume available memory and resources which over time cause computer to slow down. Refreshing the computer's resources at least once a week, will keep it running at an optimal speed with fewer problems in the long term.
5. All technology devices used by a technology user to connect to the City's networks shall continually execute approved security software with a current virus definition file. This includes user-owned equipment attached to the City's networks through remote access technologies. The City is not responsible for providing the required security software for user-owned computers.
6. E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.
7. A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.
8. Sensitive information should not be stored on removable media unless it is required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in

accordance with ITSD Security policies regarding encryption.

9. Only software that has been approved by ITSD may be installed on City owned devices. If an employee needs to have software installed on a City owned device they must submit a request to ITSD stating the business need for the software as well as any other information relevant to justify the use of the requested software. No City employee or approved contractor or vendor will install, reproduce, distribute, transmit, download, or otherwise use any software unless such software has been approved by ITSD and properly licensed. ITSD will monitor for unapproved/unauthorized software and reserves the right to remove any software from City owned devices ITSD will maintain an approved list of software that employees can access.

Password Management

Passwords are an important element of the acceptable use of technology and associated information security. A poorly chosen password may result in the compromise of the City's network. All technology users are responsible for taking appropriate steps to select and secure passwords. Users shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops, applications, mobile and/or other devices.

City Password requirements (at a minimum):

1. No departmental personnel, including administrative staff, shall request access to or maintain lists of other user passwords.
2. User account must use a "strong" password.

   Strong passwords are defined as:
   - At least eight characters in length
   - Not based on words in any language, slang, dialect or jargon
   - Not based on personal information, such as family names
   - Not common usage words like family, pets, friends, COSA, birthdays, phone numbers, addresses, computer terms, fantasy characters and/or common patterns like aaabbb, qwerty, zyxwvuts, 123321 or any derivation followed by a digit.
   - Contain at least one (1) each of the following
     - English uppercase (A through Z),
     - Lowercase (a through z),
     - digit (0 to 9) and
     - non-alphanumeric character (!,$,#,%)
3. All users' passwords will expire at intervals of ninety (90) days. Users will be prompted to change passwords beginning 10 days before the next expiration date. Passwords may not be re-used.
4. Passwords will be changed immediately after a security breach has been detected to the affected COSA systems.
5. As the COSA system software permits, an initial or reset password issued to a user will be valid only for the user's next log in. After that, the user must be prompted to change their password.
6. Users must enroll in the COSA Self-Service Password management system which provides expiration notifications and allows network passwords to be reset from desktop, laptop or mobile device.
7. Password Protection Guidelines:
   - Do not write passwords down, store them on-line, or reveal them in any electronic format.
   - Do not use the same password for COSA accounts as for other accounts (i.e. social media, personal email account, banking sites, etc.).
   - Passwords must be treated as sensitive and confidential information thus do not share City passwords with anyone.
   - ITSD support personnel may require a user to enter their password in order to resolve a problem.

- Do not talk about a password in the presence of others.
- Do not hint at the format of a password ("my family name").
- Do not click on links in emails from unknown sources; look for the "External" tag to identify email from outside of COSA.
- Do not provide account information that includes personal information and/or password.
- Do not reveal a password on questionnaires or security forms.
- Do not use the "remember password" feature.
- Do not store passwords in a file on ANY computer system without encryption.

8. COSA passwords are not to be reused or similar to any non-work related passwords for accounts such as personal email accounts or social media accounts
9. Technology users shall report any suspected security violations or threat to the ITSD Service Desk immediately. Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that technology user.

Retention and Disposition of Email

The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series All Email sent or received by a government is considered a government record. Therefore, all electronic messages must be retained and disposed of according to the City's retention requirements as described in Records Management: A.D 1.34: Records Management for Physical Electronic Records. Full detail of A.D. 1.34 can be sourced from Office of the City Clerk or **http://www.sanantonio.gov/hr/admin_directives/index.asp** . Users and their supervisors or sponsor should seek guidance from the City's Records Management Officer if there is a question concerning whether an electronic message should be deleted.

1. Electronic Mail (E-mail), Instant Messaging, Voicemail, and Text Messaging:

a. All electronic mail messages, instant messages, voicemail and text messages regarding City business must be retained and disposed of according to the City's retention requirements. It is the content and function of the record that determines the retention period for that message (A.D.1.34).

b. The City's electronic mail system is not a records management system. Electronic messages that the user determines, based on the Local Government Records Retention Schedules, are subject to retention for more than 30 days should be moved from the user's "Inbox" and/or "Sent Items" folders within 30 days of its receipt or creation. Emails in deleted folder will be purged after 14 days and electronic messages will be automatically deleted after 1 year. Electronic messages to be retained longer than 1 year may be placed in folders and saved on a network drive, or transferred to an automated records management software application.

Acceptable Use of Electronic Signatures and Electronic Records

Electronic signatures, an automated function that replaces a handwritten signature with a system generated signature statement, and electronic records can be utilized as a means for authentication of City documents, computer generated City documents and/or electronic City entries among other uses. System generated electronic signatures are considered legally binding as a means to identify the author of record for entries and confirm that the contents of what the author intended. City departments and staff will be allowed to utilize electronic signature in accordance with this directive, City, State, and/or Federal regulations regarding such.

Acceptable Use of Electronic Records and Electronic Signatures are allowed:

1. Where policies, laws, regulations, and rules require a signature and that requirement is met if the document contains an electronic signature.

2. Where policies, laws, regulations, and/or rules require a written document and that requirement is met if the document is an electronic record.
3. Where each party to a transaction must agree to conduct the transaction electronically in order for the electronic transaction to be valid and binding. Consent may be implied from the circumstances, except with respect to any electronic records used to deliver information for which consumers are otherwise entitled by law to receive in paper or hardcopy form.
4. If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner specified by law.
5. If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law.
6. If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in a record that accurately reflects the information set forth in the original record and shall remain accessible for later reference. When the requirements for retention require an original form, retention by an "electronic form" shall provide and satisfy the retention requirement.

Procedures, Forms, Guidelines and Resources for electronic signatures:

1. Procedures for electronic signatures can be found under the Texas Uniform Electronic Transactions Act
2. United States governance can be found in 18 USC 2510, Electronic Communications Privacy Act
3. Record management for COSA is established by Local Government Code: 201 through 205. The Texas State legislature requires local governments to establish a records program by Ordinance.
4. City of San Antonio adopted Ordinance 70508 and 72054
5. Ordinance 70508 (11-02-1989) names the City Clerk as the City's Record Management Officer
6. Ordinance 72054 (August 9, 1990) establishes the City's Records Management program
7. The charter of the City of San Antonio mandates that the City Clerk shall keep the records of the Council and of the City
8. Pursuant to Article II, Section 10 of the City Charter, the City Clerk shall keep the records of the Council and of the City. Pursuant to City Ordinance 72054 which establishes the City's records management program in compliance with the Local Government Records Act and reaffirms City Ordinance 70508 naming the City Clerk as the City's Records Management Officer, both ordinances filed with the Texas State Library and Archives Commission, the Records Management Officer shall develop policies and procedures in the administration of the City's records management program.
9. This policy does not supersede any local, state or federal laws regarding records management, confidentiality, information dissemination or standards of conduct.

Electronic Transactions and Signed Records:

1. Electronic Records - The Uniform Electronic Transactions Act (UETA) was enacted into law in Texas by the 77th Legislature (Senate Bill 393) in May 2001, and became effective on January 1, 2002. UETA provides definitions for several key terms that pertain to this policy. These terms are listed in the "Definition" section of this directive.
2. Electronic Signatures - Texas law (Government Code, Section 2054.60, provides a definition for the term "digital signature," which is sometimes used interchangeably with "electronic signature" (see Section II, C, 3).

Unacceptable Use of COSA Resources and the Internet

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable uses of COSA information technology systems:

1. The registration or use of any COSA related email addresses for personal accounts such as personal Email, Social Network accounts (Facebook, Twitter, LinkedIn, etc.), personal billing services (utilities, cell phone, cable, insurance, cloud based services, etc.) or any other non-work related sites.
2. Engaging in any activity that is illegal under local, state and/or federal statutes as well as any activity that violates COSA policies and Administrative Directives.
3. Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate speech. This includes any images, text, files, etc. sent electronically to co-workers or outside parties. Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden.
4. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails in most instances, not the intent of the sender. Harassment may be construed as any written, verbal or physical conduct designed to threaten, intimidate, coerce, taunt or bully the recipient or another individual.
5. Any personal use that interrupts City business and that keeps an employee from performing his/her work.
6. City systems shall not be used to chat online, "blog", or shop online if not authorized by Department Director as part of the users job function.
7. Extensive personal use of the Internet for any non-work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's Internet facilities.
8. Violating any copyright, trade secret, patent and/or other intellectual property or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.
9. Unauthorized downloading of and/or distributing of copyrighted materials.
10. Revealing a City account password to others or allowing use of a City account by others. This includes household members, coworkers, vendors, contractors and visitors when work is being done at home. Revealing a City account password to an authorized technician during a troubleshooting procedure is not a violation of this policy. In such a situation, a new password should be established as soon as possible, after the problem is resolved.
11. Requesting a password to another users network or application account.
12. Unauthorized reading, deleting, copying, modifying, printing and/or forwarding of electronic communications of another, or accessing electronic files of another without authorization.
13. Unauthorized duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Copying or installing copyrighted software for which the City or the end user does not have an active license is not permitted.
14. Sending SPAM to either internal or external parties. Individual email accounts will be limited by technical controls as a preventive measure to detect SPAM originating from a City email account. Large volume emails to recipients will not be allowed from individual email accounts. Request for approved email accounts designated for such business purposes will be submitted to ITSD Customer Service.
15. Approved email accounts must not regularly send bulk emails unless distribution lists are maintained. All undeliverable or invalid addresses from distribution lists must be regularly removed to prevent the City from not being able to send email through Internet Service Providers and/or mail hosts.

16. Downloading and/or copying music, photographs or video material, including such material that has been obtained legally, onto City computers or servers.
17. Downloading and/or installing executable program files from external media or the Internet without the approval of ITSD.
18. Exporting software, technical information, encryption software and/or technology, in violation of international or regional export control laws.
19. Using the City's electronic mail or Internet systems for private gain or profit.
20. Using unauthorized personal software which allows peer-to-peer communications between two workstations (Yahoo Messenger, Skype, Snapchat, Periscope, Instagram, Facebook Messenger, etc.).
21. Using instant messaging through public service providers.
22. Using City systems for non-work-related access to online auctions or ecommerce sites (such as e-Bay, Amazon).
23. Maliciously introducing malware or similar programs into the network or server.
24. Soliciting for political, religious, and/or other non-business uses not authorized by COSA.
25. Making fraudulent offers of products or services originating from any City account.
26. Accessing non-business related streaming media, including Internet-based radio.
27. Accessing any non-business related application which maintains a persistent application connection to the Internet, such as streaming videos or media, such as Pandora, Netflix, and/or Google Video, among others.
28. Using City technology, electronic mail and/or Internet facilities for political activity including voting, private gain, gambling, shipping, games, entertainment or other non-business function unless permitted by this directive.
29. Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department.
30. Using the COSA email system to automatically forward COSA email to a non-city email account is prohibited.
31. Sending or forwarding junk e-mail, chain letters, or other mass mailings.
32. Causing security breaches or disruptions of City communications. Security breaches or disruptions can include, but are not limited to:

    - Accessing data which the user is not authorized to access or logging into a server or user account that the user is not expressly authorized to access
    - Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service of any kind, and forged routing information for malicious purposes
    - Port scanning or vulnerability scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. ITSD should be notified prior to any such scanning
    - Circumventing user authentication or security of any device, network or account
    - Maliciously interfering with or denying service through a denial of service attack, or by other means
    - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, and/or disable, another user’s device or session, via any means, locally or via the City’s network
    - Adding/removing hardware components, attaching external devices, and/or making configuration changes to information technology devices without the explicit approval by ITSD
    - Storing confidential data on personally owned devices.

Privacy and Monitoring

1. City systems may be monitored by ITSD to support operational, maintenance, auditing, security and/or investigative activities including enforcement of this Directive, legal requests, and public records requests or for other business purpose.
2. Only Department Directors or higher may request monitoring of City administered IT systems for employees under their supervision for administrative purposes. Unauthorized monitoring or reading of electronic communications systems or their contents violates this Directive.
3. Any request to monitor must be approved by the CIO or his/her designees as well as the Human Resources (HR) Director or higher.
4. To obtain the necessary authorization, a written request from the requestor's Department Director to the HR Director must include subject employee information (i.e. name, employee number), a specific description of request (e.g. Email, share drives, web usage, telephone call logs and voice mail, etc.) and name and phone number of the employee in the requesting department who is responsible for coordination of the request.

The HR Director will forward the request to the CIO or designees for concurrence as well as to assign staff from ITSD to assist as necessary with any monitoring activities.

Roles & Responsibilities

Users	1. Users are required to adhere to the provisions of this AD. 2. Users should be aware that all information created, stored, or processed by a COSA information technology system is the property of the City of San Antonio. There should be no expectation of user privacy or confidentiality with regard to any files, including Email, stored on City computers. Any materials stored or processed on City information systems may be monitored and reviewed by City management at any time. In addition, users should be aware that any information processed and/or stored on any City information technology system is subject to applicable open records laws. 3. All lost equipment must be reported to the ITSD Service Desk. All stolen IT equipment shall be reported to the San Antonio Police Department (SAPD) and the associated case numbers reported to the ITSD Service Desk. COSA IT equipment can be any City-owned device, mobile device, and/or personal device that contain COSA data. In addition, all COSA capital assets that are lost or stolen shall be reported to the Finance Department in accordance with A.D. 8.7. 4. Users who voluntarily terminate employment or contract, retire, or are transferred, will be required to review their e-mail accounts with their supervisor or sponsor. The user's supervisor or sponsor is responsible for ensuring that e-mail records are properly classified and stored. All unnecessary working or convenience copies shall be disposed of appropriately.

ITSD	1. ITSD and Human Resources will provide City departments with initial communication and training regarding application of this directive. However, City Department Directors are ultimately responsible for communicating the policies established in this AD to all personnel in their respective departments and for ensuring compliance within their respective departments. 2. ITSD is responsible for publishing and disseminating the standards and procedures established to implement this directive to all relevant personnel, third-party users including (contractors, consultants, vendors, business partners etc.) and for monitoring compliance. City departments who work with third-party users are responsible for identifying the third-party users to ITSD upon on boarding and terminating. 3. ITSD is responsible for ordering, inventorying, managing, and supporting all of the City's information technology assets, which includes, but not limited to, desktops, laptops, tablets, mobile phones, servers, software, mobile applications, networking equipment, and printers. 4. Any computer-based device may be disconnected from the City network at any time, if continued connectivity constitutes a threat to the City or any City-administered information technology system. ITSD will attempt to contact the business owner responsible for the computer prior to disconnecting as long as such notification does not allow further degradation of the City-administered information technology systems. Such notification will be made after the disconnection, if prior coordination was not possible. 5. User's access may be terminated if he/she is found in breach of this directive. Service may be restored to the user following a written request by the user's Department Director or sponsor. 6. ITSD may isolate a sender's email message from reaching a user's City e-mail account. The following process must be followed in order to isolate email messages sent to the City's email system: 7. A user who receives repeated or multiple unsolicited, unacceptable annoying, alarming, abusive, embarrassing or offensive e-mail messages from a sender outside of the City must request the sender to stop sending such messages and inform the sender that any emailed requests for City records or documents must be sent to the City's Officer for Public Information at: http://www.sanantonio.gov/opengovernment. 8. The user must provide copies of the messages and all correspondence between the user and sender, to the user's Department Director or appropriate Executive Leadership Team (ELT) member along with a written request to have ITSD isolate the sender's e-mails. 9. The Department Director or ELT member and the Office of the City Attorney will review the request and determine if the request is warranted. 10. It the request is deemed warranted and subsequently approved, it will be submitted to ITSD Customer Service for email isolation. 11. ITSD will work with Human Resources to provide a security awareness training program annually to City employees.

Department Directors and their Designees	1. Departments are responsible for implementation, training, and enforcement of the data classification standards defined by the Texas State Attorney General's Office as they apply to information created, stored, or processed on City-administered technology or equipment including data retention and disposition. 2. Department Directors are responsible for any disciplinary actions taken against employees who violate this policy. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary actions to be taken against employees who violate this policy. 3. Department Directors/designee are responsible for requesting all IT services and equipment including, desktop computer, laptop, tablet, mobile phone or other mobile IT equipment as well as access to non-departmental data. 4. IT assets requested by Department Directors will be assigned to the department in the COSA asset management system. Director/designee and the user receiving equipment will be required to complete all necessary forms accepting accountability for equipment and will be responsible for use and protection of asset. 5. Upon the voluntary or involuntary termination of any department employee or non-employee with system or physical access, or upon notification of such termination, the Department will notify HR and ITSD to ensure access authorizations are revoked. Department will take custody of, or ensure the safe return, modification, or destruction of the following items assigned, or relating, to the terminating or notified person: • Keys, parking passes/cards, and identification badges. • Change lock combinations and passwords that would have been used by terminated user on department managed systems not accessed through their network password. • Collect sensitive documentation, along with operator procedures, and other documentation and manuals. • Notify ITSD prior to any reassignment of COSA owned computers, mobile devices, software or other IT assets. 6. Department Directors will be provided a biannual departmental IT equipment inventory for discrepancy reconciliation.
Office of the City Clerk	1. The Records Management Officer will, in cooperation with ITSD, ensure that appropriate training and communication, retention, maintenance, and disposition requirements for applicable information are in accordance with AD 1.34 Paper, Microfilm, and Electronic Records Management. 2. Responsible for the creation, maintenance and administration of all rules regarding the classification and protection of applicable information stored on City-administered information technology systems.

Human Resources	1. Human Resources Department is responsible for providing accurate job descriptions and requiring security responsibilities to be addressed in the terms and conditions of employment. Candidates for employment will be adequately screened, especially for positions of trust. Furthermore, management will require employees, contractors and other users, to apply security in accordance with established policies and procedures. 2. Human Resources will provide guidance to department for disciplinary actions associated with violations of the directive. 3. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. New employees are provided a copy of this directive and users with network and application access are enrolled in security awareness training which includes an acknowledgment regarding the acceptable use of COSA technology. 4. The HR Director will consult with the Chief Information Officer (CIO) or his/her designee in approving any monitoring of systems for personnel administration purposes.

Discipline

Compliance with COSA administrative directives, security policies, and/or procedures is the responsibility of all COSA employees, contractors and/or other third parties. The City can temporarily or permanently suspend, block, and/or restrict access to information or physical assets, independent of such procedures, when it is reasonable and associated probable cause exists to do so in order to protect the confidentiality, integrity or availability of City resources as well as protect the City from liability, and/or to comply with applicable federal, state, and municipal laws, regulations, statutes, court orders, or other contractual obligations. Violations of any of these directives shall result in disciplinary actions in accordance with section 2 of Rule XVII of the Municipal Civil Service Rules for civilian employees, or in accordance with Chapter 143 of the Texas Local Government Code and current respective Collective Bargaining Agreement for uniformed employees covered under collective bargaining agreements. Administrative action may range from reprimand and loss of access privileges to suspension to separation of employment. Violations may also result in civil and/or criminal prosecution.

RFCSP ATTACHMENT G

THIRD PARTY VENDOR IT CLOUD SECURITY QUESTIONNAIRE

The appropriate questionnaire must be filled out and returned with the proposal if solution proposed is Software as a Service (SaaS). This questionnaire is not required for proposals consisting of on-premise solutions.

Please choose the appropriate questionnaire to complete based on the platform hosting the solution proposed:

AWS: Attachment G.1

Azure: Attachment G.2

Google: Attachment G.3

All other cloud platforms: Attachment G.4

All four questionnaires are attached to this document.

CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

Cloud Security Assessment Questionnaire

for Vendors(Amazon Web Services -AWS)

Version **4**.0 0**7/01/2020**

Table of Contents

Overview

This document will be used as a preliminary questionnaire to allow Information Technology Services Department (ITSD) Security Group to assess the physical, logic and security administration controls used by a third party application service provider or business partner.

Assessment Process

Identification of Parties Involved

The following are the four groups involved in this assessment process:

Group Name	Role
ITSD Security	Initiator of Process, Performs Assessment, Reports Findings/Risk Recommendation
Project Manager	Coordinates interaction between ITSD and external vendors.
-Vendor/Company-	Provides answers to questionnaire.
CSO	Makes Risk Recommendation
Business Owner	Accepts Final Report

Area 1	Certifications, Programs, Reports, and Third-Party Attestations	
01	AWS GovCloud? What Region of GovCloud? (AWS GovCloud (US-West) or AWS GovCloud (US-East)	(Select One)
02	Project is associated with CJIS, PCI or HIPAA Data?	(Select One)
03	What Type of VPN Connection established with AWS (Ex AWS Site-to-Site VPN, AWS Client VPN, AWS VPN Cloud-Hub, Third party software VPN appliance and AWS Direct Connect)	(Select One)
04	How many COSA users are configured AWS (IAM) ?	(Select One)
05	Who is responsible for Monitoring VPN Connection and do we have access to see Amazon VPC Dashboard (VPN tunnel status, Site-to-Site VPN connections)?	(Select One)
06	Vendor signed with AWS CloudTrail & AWS Cloud watch?	(Select One)
07	How much assistance will the vendor provide COSA with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	(Select One)

Area 2	Select the Security, Identity, & Compliance Tools Implemented for the Project		Response
09	AWS Identity and Access Management	(Identity and Access Control)	(Select One)
10	AWS Artifact	Security and compliance documents (AWS ISO certifications, PCI, and SOC).	(Select One)
11	Amazon Cognito	(User pools and identity pools)	(Select One)
12	Amazon Detective	(Identify the root cause of security findings or suspicious activities)	(Select One)
13	AWS Directory Service	(Identity and Access Control)	(Select One)
	AWS Firewall Manager		(Select One)
14	AWS Cloud Directory		(Select One)
15	AWS Cloud Trail	(Monitoring and Logging)	(Select One)
16	Amazon Cloud Watch	(Monitoring and Logging)	(Select One)
17	Amazon GuardDuty	(Monitoring and Logging)	(Select One)
18	Amazon Inspector		(Select One)
19	Amazon Macie		(Select One)
20	AWS Resource Access Manager		(Select One)
21	AWS Secrets Manager		(Select One)
	AWS Security Hub		(Select One)
	AWS Shield		(Select One)
22	AWS Single Sign-On	(Identity and Access Control)	(Select One)
	AWS WAF		(Select One)

Specify any other Security Tools Integrated with AWS Cloud:

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1	Will the services provided to COSA include Data-as-a-Service (DaaS)? *Data is provided to COSA through specific interfaces.*	(Select One)
2	Will the services provided to COSA include Software-as-a-Service (SaaS)? *COSA uses your applications running on your cloud infrastructure.*	(Select One)
3	Will the services provided to COSA include Platform-as-a-Service (PaaS)? *COSA deploys onto your cloud infrastructure COSA-created or acquired applications created using programming languages, libraries, services, and tools supported by you.*	(Select One)
4	Will the services provided to COSA include Infrastructure-as-a-Service (IaaS)? *COSA is able to deploy and run arbitrary software, which can include operating systems and applications, on processing, storage, networks, and other fundamental computing resources you provide.*	(Select One)
5	Does the application support per-client security controls:	(Select One)
6	Password complexity requirements?	(Select One)
7	Password length requirements?	(Select One)
8	Password expiration?	(Select One)
9	Password history requirements?	(Select One)
10	Account lockout due to failed access attempts? (maximum of six)	(Select One)
11	Are passwords masked while entered?	(Select One)
12	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc.) for user access?	(Select One)
13	Can the application login screen be restricted to the COSA network IP range?	(Select One)
14	Does the application require transport encryption? (SSL)	(Select One)
15	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
16	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
17	Has the application been inspected for database injection attacks?	(Select One)
18	Have identified database injection vulnerabilities been remediated?	(Select One)
19	Has the application been inspected for session hijacking attacks?	(Select One)
20	Have identified session hijacking vulnerabilities been remediated?	(Select One)
21	Has the application been inspected for buffer overflow attacks?	(Select One)
22	Have identified buffer overflow vulnerabilities been remediated?	(Select One)
23	Does the application validate user input fields against malicious data entry?	(Select One)
24	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
25	Does the application restrict account administration through the website?	(Select One)
26	Does the application restrict system administration through the website?	(Select One)
27	Has the application been cleansed of built-in sample application code? (scripts)	(Select One)
28	Has the application been cleansed of built-in sample data?	(Select One)
29	Is application security assessed on a periodic basis?	(Select One)

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
30	Is the assessment performed by an external security consultant or company?	(Select One)
31	Is the assessment performed annually?	(Select One)
32	Is a security assessment performed after major upgrades to the application?	(Select One)
33	Are issues identified by a security assessment remediated?	(Select One)
34	Do you have the ability to logically segment customer data so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	(Select One)
35	Can you provide the physical location of storage of a tenant's data upon request?	(Select One)
36	Do you allow tenants to define acceptable geographical locations for data routing or data storage?	(Select One)
37	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
38	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
39	Can you provide a documented procedure on how tenant data is sanitized from your systems once the service contract/relationship ends?	(Select One)
40	Do you "data mine" tenant data for your company's benefit?	(Select One)
41	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	

CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

Cloud Security Assessment Questionnaire for Vendors (Microsoft Azure)

Version 4.0 07/01/2020

Table of Contents

Overview

This document will be used as a preliminary questionnaire to allow Information Technology Services Department (ITSD) Security Group to assess the physical, logic and security administration controls used by a third party application service provider or business partner.

Assessment Process

Identification of Parties Involved

The following are the four groups involved in this assessment process:

Group Name	Role
ITSD Security	Initiator of Process, Performs Assessment, Reports Findings/Risk Recommendation
Project Manager	Coordinates interaction between ITSD and external vendors.
-Vendor/Company-	Provides answers to questionnaire.
CSO	Makes Risk Recommendation
Business Owner	Accepts Final Report

Area 1	Certifications, Programs, Reports, and Third-Party Attestations	
1.	Azure GovCloud? What Region of GovCloud? (US Gov Arizona, Texas or Virginia)	(Select One)
2.	Project is associated with CJIS, PCI or HIPAA Data?	(Select One)
3.	What Type of virtual network is created with Azure (Ex: Portal, PowerShell or Azure CLI)	(Select One)
4.	Who is responsible “Security controls for Azure VPN Gateway and Azure Vnet”? (ex-tools: Azure Monitor Log Analytics; Azure VPN Gateway metrics) COSA or Vendors?	(Select One)
5.	COSA users are configured Azure Active Directory (IAM)?	(Select One)
6.	How much assistance will the vendor provide COSA with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	(Select One)

Area 2	Select the Security, Identity, & Compliance Tools Implemented for the Project	Response
7.	Azure Identity and Access Management (Identity and Access Control) Azure AD	(Select One)
8.	Azure Firewall	(Select One)
9.	Azure DDoS Protection	(Select One)
10.	Azure NetApp Files	(Select One)
11.	Azure Network-based anomaly detection	(Select One)
12.	Azure adaptive application controls	(Select One)
13.	Azure Web filtering	(Select One)
14.	Microsoft Endpoint Protection for Azure	(Select One)
15.	Azure Vulnerability management (Qualys Scanner)	(Select One)
16.	**Specify any other Security Tools Integrated with Azure Cloud:**	

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1.	Will the services provided to COSA include Data-as-a-Service (DaaS)? *Data is provided to COSA through specific interfaces.*	(Select One)
2.	Will the services provided to COSA include Software-as-a-Service (SaaS)? *COSA uses your applications running on your cloud infrastructure.*	(Select One)
3.	Will the services provided to COSA include Platform-as-a-Service (PaaS)? *COSA deploys onto your cloud infrastructure COSA-created or acquired applications created using programming languages, libraries, services, and tools supported by you.*	(Select One)
4.	Will the services provided to COSA include Infrastructure-as-a-Service (IaaS)? *COSA is able to deploy and run arbitrary software, which can include operating systems and applications, on processing, storage, networks, and other fundamental computing resources you provide.*	(Select One)
5.	Does the application support per-client security controls:	(Select One)
6.	Password complexity requirements?	(Select One)
7.	Password length requirements?	(Select One)
8.	Password expiration?	(Select One)
9.	Password history requirements?	(Select One)
10.	Account lockout due to failed access attempts? (maximum of six)	(Select One)
11.	Are passwords masked while entered?	(Select One)
12.	Can the application login screen be restricted to the COSA network IP range?	(Select One)
13.	Does the application require transport encryption? (SSL)	(Select One)
14.	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
15.	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
16.	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
17.	Does the application restrict account administration through the website?	(Select One)
18.	Is application security assessed on a periodic basis?	(Select One)

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1.	Is the Security assessment performed by an external security consultant or company?	(Select One)
2.	Is the Security assessment performed annually?	(Select One)
3.	Is a security assessment performed after major upgrades to the application?	(Select One)
4.	Do you have the ability to logically segment customer data so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	(Select One)
5.	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
6.	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
7.	Do you “data mine” tenant data for your company’s benefit?	(Select One)
8.	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	

CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

Cloud Security Assessment Questionnaire for Vendors(Google Cloud -GCP)

Version 4.0 07/01/2020

Table of Contents

Overview

This document will be used as a preliminary questionnaire to allow Information Technology Services Department (ITSD) Security Group to assess the physical, logic and security administration controls used by a third party application service provider or business partner.

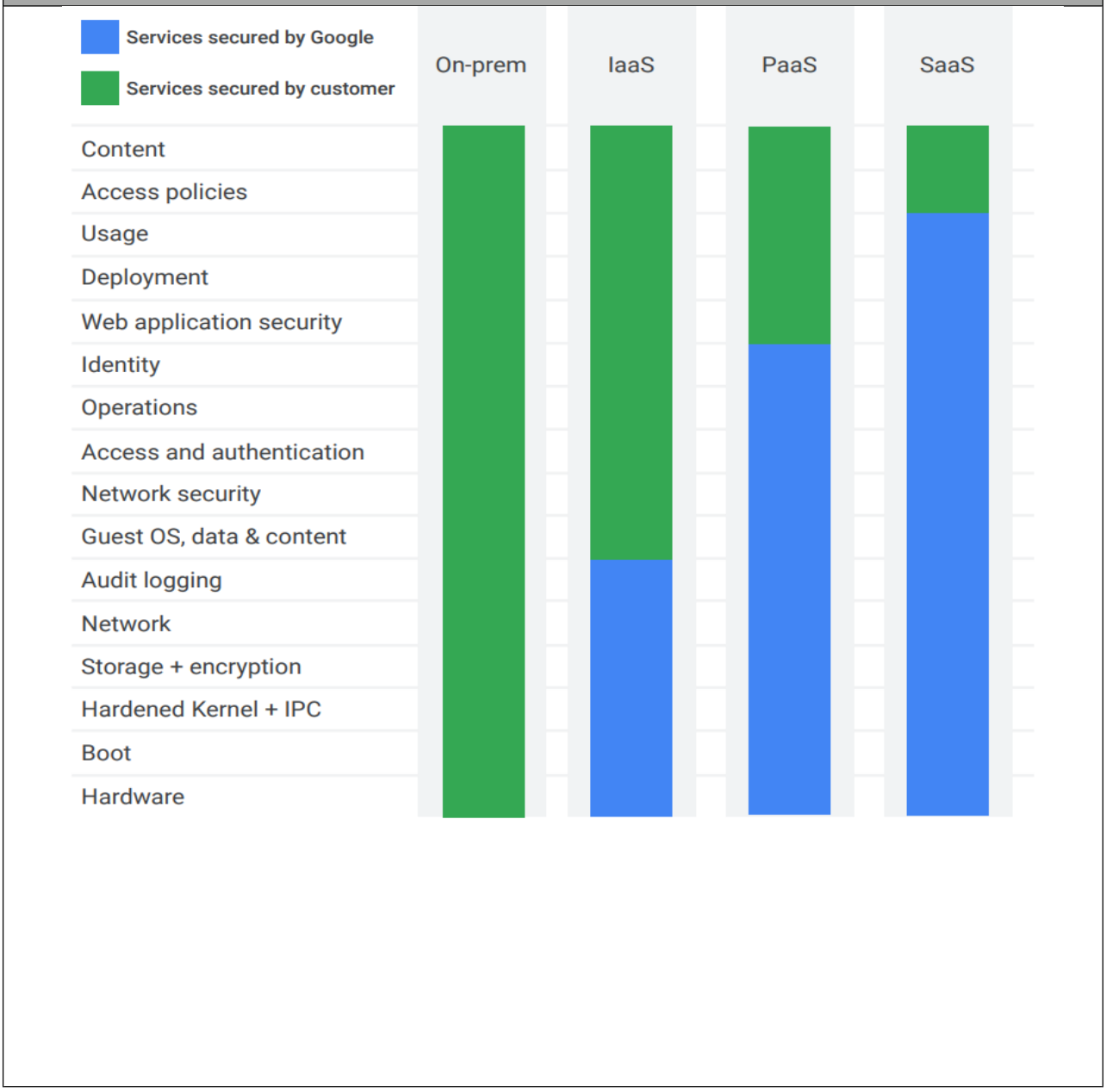
Assessment Process

Identification of Parties Involved

The following are the four groups involved in this assessment process:

Group Name	Role
ITSD Security	Initiator of Process, Performs Assessment, Reports Findings/Risk Recommendation
Project Manager	Coordinates interaction between ITSD and external vendors.
-Vendor/Company-	Provides answers to questionnaire.
CSO	Makes Risk Recommendation
Business Owner	Accepts Final Report

3. RESPONSIBILITY CHART: GCP Vs CLOUD VENDOR(Customer)



Area 1	Certifications, Programs, Reports, and Third-Party Attestations	Response
1.	GCP GovCloud? What Region of GovCloud?	(Select One)
2.	Project is associated with CJIS, PCI or HIPAA Data?	(Select One)
3.	CSA Consensus Assessments Initiative Questionnaire v3.0.1. Registered and answered	(Select One)
4.	VPC Service Controls is defined ? Security perimeter around Google Cloud Platform resources such as Cloud Storage buckets, Bigtable instances, and BigQuery datasets established ?	(Select One)
5.	COSA users are configured (IAM)?	(Select One)
6.	Security Command Center With Standard tiers or Premium tier Features ? (STD-Security Health Analytics and Web Security Scanner) (Premium -Event Threat Detection,Container Threat Detection and Web Security Scanner	(Select One)
7.	GCP Cloud Data Loss Prevention(DLP) Feature Avialbale ?	(Select One)
8.	How much assistance will the vendor provide COSA with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	(Select One)

Area 2	Select the Security, Identity, & Compliance Tools Implemented for the Project	Response
9.	GCP Identity and Access Management (Identity and Access Control)	(Select One)
10.	Cloud Armor (Protect your applications and websites against denial of service and web attacks)	(Select One)
11.	Access Transparency (Access Transparency provides logs of the actions taken by Google personnel)	(Select One)
12.	GCP Cloud Audit Logs-	(Select One)
13.	GCP Cloud Key Management Service-is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises.	(Select One)
14.	Data incident response	(Select One)
15.	**Specify any other Security Tools Integrated with GCP Cloud:**	

NOTE: The following section is for third party service providers of web-based resources.

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1.	Will the services provided to COSA include Data-as-a-Service (DaaS)? *Data is provided to COSA through specific interfaces.*	(Select One)
2.	Will the services provided to COSA include Software-as-a-Service (SaaS)? *COSA uses your applications running on your cloud infrastructure.*	(Select One)
3.	Will the services provided to COSA include Platform-as-a-Service (PaaS)? *COSA deploys onto your cloud infrastructure COSA-created or acquired applications created using programming languages, libraries, services, and tools supported by you.*	(Select One)
4.	Will the services provided to COSA include Infrastructure-as-a-Service (IaaS)? *COSA is able to deploy and run arbitrary software, which can include operating systems and applications, on processing, storage, networks, and other fundamental computing resources you provide.*	(Select One)
5.	Does the application support per-client security controls:	(Select One)
6.	Password complexity requirements?	(Select One)
7.	Password length requirements?	(Select One)
8.	Password expiration?	(Select One)
9.	Password history requirements?	(Select One)
10.	Account lockout due to failed access attempts? (maximum of six)	(Select One)
11.	Are passwords masked while entered?	(Select One)
12.	Can the application login screen be restricted to the COSA network IP range?	(Select One)
13.	Does the application require transport encryption? (SSL)	(Select One)
14.	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
15.	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
16.	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
17.	Does the application restrict account administration through the website?	(Select One)
18.	Is application security assessed on a periodic basis?	(Select One)

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
19	Is the Security Compliance assessment performed by an external security consultant or company? ex- SOC-1/SOC-2/SOC-3,CSA, ISO-9001,27001,27017,27018) Report	(Select One)
20	Security assessment performed annually?	(Select One)
21	Security assessment performed after major upgrades to the application?	(Select One)
22	Do you have the ability to logically segment customer data so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	(Select One)
23	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
24	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
25	Do you “data mine” tenant data for your company’s benefit?	(Select One)
26	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	

CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

IT Security **Cloud** Questionnaire

07/01/2020

Table of Contents

Overview

This document will be used as a preliminary questionnaire to allow Information Technology Services Department (ITSD) Security Group to assess the physical, logic and security administration controls used by a third party application service provider or business partner.

Assessment Process

Identification of Parties Involved

The following are the four groups involved in this assessment process:

Group Name	Role
ITSD Security	Initiator of Process, Performs Assessment, Reports Findings/Risk Recommendation
Project Manager	Coordinates interaction between ITSD and external vendors.
-Vendor/Company-	Provides answers to questionnaire.
CSO	Makes Risk Recommendation
Business Owner	Accepts Final Report

Questionnaire

INSTRUCTIONS
The following questionnaire targets nine areas for the purpose of information gathering and assessment. In order to expedite and simplify the process, questions have been constructed for a Yes/No/N/A response. Space has been provided in each section for additional information if needed.

Area 1	SECURITY POLICY	Response
1	Does your company have an information security policy approved by senior management?	(Select One)
2	Has the security policy been published and communicated to all constituents?	
3	Indicate if the following topics are covered by your policies:	(Select One)
4	Computer and communications systems access and use?	
5	Employee accountability?	(Select One)
6	Business Continuity?	
7	Remote access?	(Select One)
8	Physical access?	
9	Email?	(Select One)
10	Encryption?	
11	Operating system security?	(Select One)
12	Access control?	
13	Change control?	(Select One)
14	Security incident management?	
15	Personnel security and termination?	(Select One)
16	Security awareness?	
17	Risk management?	(Select One)
18	Do your information security and privacy policies align with any particular industry standards (NIST 800-53, ISO-27001, ISO-22307, CoBIT, etc.)?	(Select One)
	Additional Information:	

Area 2	ORGANIZATIONAL	Response
1	Is there an individual or group with responsibility for information security within the organization to ensure compliance to the policy and process?	(Select One)
2	Are all constituents required to sign confidentiality agreements?	(Select One)
3	Do your contracts with third party service providers who may have access to target data include the following:	(Select One)
4	Confidentiality agreement	(Select One)
5	Non-Disclosure Agreement	(Select One)
6	Compliance with security standards	(Select One)
7	Right to audit	(Select One)
8	Notification of change	(Select One)

Area 2	ORGANIZATIONAL	Response
9	Breach Notification	(Select One)
10	Privacy requirements	(Select One)
11	Employee and contractor screening practices	(Select One)
12	Business Continuity/Incident Response requirements	(Select One)
13	Is a process in place to regularly monitor your 3rd party service providers to ensure compliance with security standards?	(Select One)
14	Is an awareness program in place to communicate your security standards and expectations to 3rd party service providers?	(Select One)
15	Are documented procedures in place for the disposal and/or destruction of physical media (e.g.: Paper documents, CDs, DVDs, tapes, disk drives, etc.)?	(Select One)
16	Are documented procedures in place for the reuse of physical media (e.g.: Tapes, disk drives, etc.)?	(Select One)
17	Does the site have a current SSAE-16 SOC 2 report available?	(Select One)
18	Can the site provide a copy of the report to COSA?	(Select One)
19	Does the service provider maintain a technical support hotline?	(Select One)
20	Is the support line available 24 hours a day?	(Select One)
21	Is the support line available 7 days a week?	(Select One)
22	Do you use industry standards to build in security for your Systems/Software Development Lifecycle (SDLC)?	(Select One)
23	Do you participate or subscribe to an information security threat intelligence service?	(Select One)
	Additional Information:	

Area 3	HUMAN RESOURCES	Response
1	Does your company use an external background screening agency?	(Select One)
2	Do applicants undergo background checks prior to being hired?	(Select One)
3	Do contractors / third parties undergo background checks prior to being hired?	(Select One)
4	Does your HR department notify security / access administration of employee change of status/termination in a timely manner?	(Select One)
5	Is the access for terminated employees removed immediately upon notification?	(Select One)
6	Do you notify security / access administration of contractor, business partner or third-party change of status/termination in a timely manner?	(Select One)
7	Is the access for terminated contractors, business partners or third parties removed immediately upon notification?	(Select One)
8	Is there a process in place for the return of assets (laptop, desktop, PDA, cell phones, access cards, tokens, smart cards, keys, proprietary documentation) for changed status/terminated constituents?	(Select One)
	Additional Information:	

Area 4	PHYSICAL / ENVIORNMENTAL	Response
1	Do the perimeters surrounding the target systems contain the following elements:	(Select One)
2	Motion sensors at entry points in the data center?	(Select One)
3	Closed circuit camera pointed at entry points in the data center?	(Select One)
4	Are unattended system displays and consoles locked?	(Select One)
5	Security guards at points of entry?	(Select One)
6	Secured / Locked cabinets?	(Select One)
7	Badge readers at points of entry?	(Select One)
8	Biometric readers at points of entry?	(Select One)
9	Locked doors requiring a key or PIN at points of entry?	(Select One)
10	Single point of entry?	(Select One)
11	External lighting?	(Select One)
12	Security patrols?	(Select One)
13	Alarms on exterior doors?	(Select One)
14	Alarms on windows?	(Select One)
15	Do emergency-specific doors only permit external egress?	(Select One)
16	Are all visitors always escorted when inside the facility?	(Select One)
17	Are visitors required to sign in and out?	(Select One)
18	Is there a process in place for requesting, approving and granting access to restricted secure areas?	(Select One)
19	Is a process in place to periodically review access to restricted secure areas?	(Select One)
20	Is there a segregation of duties between those responsible for the storage and the granting of access devices (e.g.: badges, keys, etc.)?	(Select One)
21	Is there segregation of duties in granting and approving access to restricted secure areas?	(Select One)
22	Is a list maintained of all personnel possessing cards / keys to the data center?	(Select One)
23	Are access badges two factor authentication (PIN in combination with the card)	(Select One)
24	Is a process in place to report lost access cards / keys?	(Select One)
25	Is a process in place to periodically review access to restricted secure areas?	(Select One)

Area 4	PHYSICAL / ENVIORNMENTAL	Response
26	Are CCTV images stored and retained?	(Select One)
27	Is the facility (ies) that contain the target systems monitored 24x7x365?	(Select One)
28	Does the hardware for the target systems in the perimeter contain the following physical elements:	(Select One)
29	Backup generator?	(Select One)
30	Fluid or water sensor?	(Select One)
31	Heat detector?	(Select One)
32	Smoke detector?	(Select One)
33	Thermostat?	(Select One)
34	Uninterruptible Power Supply (UPS)?	(Select One)
35	Fire suppression?	(Select One)
36	Multiple power feeds?	(Select One)
37	Multiple communication feeds?	(Select One)
38	Is your facility serviced by external redundant power sources?	(Select One)
39	Is access to the communication cabling termination areas restricted to authorized employees only?	(Select One)
	Additional Information:	

Area 5	COMMUNICATIONS / OPERATIONS	Response
1	Are there a formal change management / change control policy and process in place?	(Select One)
2	Is separation of duties enforced between those approving a change and those implementing the change?	(Select One)
3	Are change control logs maintained?	(Select One)
4	Are there different source code repositories for production and non-production code?	(Select One)
5	Is the production environment logically segregated from the non-production environments?	(Select One)
6	Do you have procedures in place to ensure production data shall not be used in non-production environments?	(Select One)
7	Third Party Management:	(Select One)
8	Is your company the sole provider of all aspects of this service (not outsourced)?	(Select One)
9	Are third party vendors restricted from accessing target data (backup vendors, service providers, equipment support, etc.)?	(Select One)
10	Are confidentiality agreements in place?	(Select One)
11	Are non-disclosure agreements in place?	(Select One)
12	Are third parties required to notify you of any changes that may affect services rendered?	(Select One)
13	Anti Virus:	(Select One)
14	Is there an anti-virus / malware solution deployed on servers?	(Select One)
15	Is there an anti-virus / malware solution deployed on desktops?	(Select One)
16	Is on-access / real-time scanning enabled?	(Select One)
17	Are systems automatically checked for new signature updates and updated?	(Select One)
18	Is there a process to facilitate emergency anti-virus signature updates?	(Select One)
19	In addition to traditional signature based detection, does your company's anti-virus/anti malware capability include:	(Select One)
20	Employee awareness training?	(Select One)
21	Software integrity checking?	(Select One)

Area 5	COMMUNICATIONS / OPERATIONS	Response
22	Anomaly/behavior monitoring?	(Select One)
23	Data Back-Up:	(Select One)
24	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	(Select One)
25	Is back-up media stored off-site?	(Select One)
26	If a third-party facility is used, are contractual obligations in place addressing the following:	(Select One)
27	Secure transport of media?	(Select One)
28	Tracking of shipments?	(Select One)
29	Verification of receipt?	(Select One)
30	Is back-up data encrypted on the back-up media?	(Select One)
31	Is access to back-up media restricted to authorized personnel only?	(Select One)
32	Do your data protection mechanisms address malicious data corruption threats; including corruption of backup data?	(Select One)
33	Network Security:	(Select One)
34	Do you conduct network-layer vulnerability scans:	(Select One)
35	Monthly?	(Select One)
36	Quarterly?	(Select One)
37	Annually?	(Select One)
38	Do you have a capability to rapidly patch vulnerabilities across all of your operating systems?	(Select One)
39	Do you have a capability to rapidly patch vulnerabilities across all of your applications?	(Select One)
40	Is every connection to an external network terminated at a firewall?	(Select One)
41	Are boundary devices configured to prevent communications from unapproved networks?	(Select One)
42	Do boundary devices deny all access by default?	(Select One)
43	Is a process in place to request, approve, log, and review access to networks across boundary devices?	(Select One)
44	Are boundary traffic events logged to support historical or incident research?	(Select One)
45	Are security patches regularly reviewed and applied to boundary devices as appropriate?	(Select One)
46	Is there an approval process prior to implementing or installing a network device at the boundary?	(Select One)
47	Do you have documented security configuration baselines for :	(Select One)
48	Perimeter defense (e.g., IDS/IPS, Firewall, etc)?	(Select One)
49	Network infrastructure (e.g., routers, switches, DNS, DC, etc.)?	(Select One)
50	Hosts/servers?	(Select One)
51	Are your security configuration baselines aligned to industry standards (CIS, NIST, etc.)?	(Select One)
52	Are network devices periodically monitored for continued compliance to security requirements?	(Select One)
53	Is a solution in place to prevent unauthorized devices from physically connecting to the internal network?	(Select One)
54	Are monitoring tools deployed and configured in critical segments to detect compromise of network or boundary device security?	(Select One)
55	Are internal users required to pass through a content filtering proxy prior to accessing the Internet?	(Select One)
56	Are internal systems required to pass through a content filtering proxy prior to accessing the Internet?	(Select One)
57	Is the network on which Internet-facing systems reside segregated from the internal network? (i.e.: DMZ)	(Select One)

Area 5	COMMUNICATIONS / OPERATIONS	Response
58	Is the DMZ limited to only those servers that require access from the Internet?	(Select One)
59	Are monitoring tools configured in the DMZ to detect compromise of network or boundary device security?	(Select One)
60	Are the logs for DMZ monitoring tools and DMZ devices stored on the internal network?	(Select One)
61	Is data on the DMZ for incoming file transfers removed on a timely basis?	(Select One)
62	Is there a separate network segment for endpoints for remote access?	(Select One)
63	Is the use of wireless networking technology prohibited in your organization?	(Select One)
64	Do you have a policy and approval process in place if wireless networking technology is allowed?	(Select One)
65	Are access points prohibited in the production environment?	(Select One)
66	Are access points physically isolated from company-owned networks?	(Select One)
67	If not, are access points located on a separate network segment?	(Select One)
68	Is this segment firewalled from the rest of the network?	(Select One)
69	Do access points filter by MAC address?	(Select One)
70	Are systems using wireless networking in the environment also allowed to connect via a secondary network connection? (e.g.: LAN cable, 2nd wireless, etc.)	(Select One)
71	Are wireless connections authenticated?	(Select One)
72	Are logins via wireless connections logged?	(Select One)
73	Are wireless connections always encrypted?	(Select One)
74	Do you regularly scan your organization's facilities for rogue wireless access points?	(Select One)
75	Intrusion Detection / Prevention:	(Select One)
76	Is a network Intrusion Detection system in place?	(Select One)
77	Is a network Intrusion Prevention System in place?	(Select One)
78	If so, is it in place on the following network segments:	(Select One)
79	Internet point-of-presence?	(Select One)
80	DMZ?	(Select One)
81	Extranet?	(Select One)
82	Internal production network?	(Select One)
83	Network segment hosting target data?	(Select One)
84	Is it configured to generate alerts in case of incidents and values exceeding normal thresholds for your environment?	(Select One)
85	Is there a formal process in place to regularly update the IDS signatures based on new threats and changes in your environment?	(Select One)
86	Is the system monitored 24x7x365?	(Select One)
87	In the event of a NIDS functionality failure, is an alert generated?	(Select One)
88	Is a host-based intrusion detection system employed in the production application environment?	(Select One)
89	Media:	(Select One)
90	Is there a policy and process in place that addresses the use and management of removable media? (e.g.: CDs, DVDs, tapes, disk drives, etc.)	(Select One)
91	Is sensitive data prohibited from residing on removable/portable media?	(Select One)
92	If sensitive data is allowed on removable/portable media is the data encrypted?	(Select One)
93	Is a documented process in place for the disposal of media?	(Select One)
94	Data Exchange:	(Select One)
95	Do you have policies and/or procedures in place that address the following forms of information exchange:	(Select One)
96	Do external file transfers requests undergo a review and approval process?	(Select One)
97	Do you leverage encryption to protect data during transport across networks?	(Select One)
98	Do you leverage encryption to protect data during transport between networks?	(Select One)

Area 5	COMMUNICATIONS / OPERATIONS	Response
99	Is a mutual authentication protocol utilized between your organization and a 3rd party to validate the integrity and origin of the data?	(Select One)
100	Are external file transfers logged?	(Select One)
101	Is there a process in place to reconcile the list of packages?	(Select One)
102	Are media transport personnel bonded?	(Select One)
103	Is instant messaging system use prohibited?	(Select One)
104	If an instant messaging system is used, is encryption used?	(Select One)
105	Is the exchange of target data or confidential information through email prohibited?	(Select One)
106	Is an email filtering solution in place?	(Select One)
107	Monitoring Logs:	(Select One)
108	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	(Select One)
109	Are logs generated for security relevant activities on :	(Select One)
110	Network devices?	(Select One)
111	Operating systems?	(Select One)
112	Applications?	(Select One)
113	Are these logs reviewed at regular intervals using a specific methodology to uncover potential incidents?	(Select One)
114	Are audit logs stored on alternate systems?	(Select One)
115	Do you protect audit logs against :	(Select One)
116	Modification	(Select One)
117	Deletion?	(Select One)
118	Inappropriate access?	(Select One)
119	Does your logging and monitoring framework allow you to identify the specific tenants affected by an incident?	(Select One)
120	Encryption:	(Select One)
121	Do you utilize industry standard encryption methodologies (PKI, AES, etc.) any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	(Select One)
122	Is target data encrypted in storage / at rest within your organization?	(Select One)
123	Is a centralized key management system in place?	(Select One)
124	Is the administration of key management handled internally?	(Select One)
125	Are symmetric keys generated in at least two parts?	(Select One)
126	If so, are parts stored on separate physical media?	(Select One)
127	Are procedures in place to prevent a single individual from having access to both parts of a symmetric key?	(Select One)
128	Are procedures in place to prevent the same key/certificate from being shared between production and non-production environments?	(Select One)
129	Are default certificates provided by vendors replaced with the company's own certificates?	(Select One)
	Additional Information:	

Area 6	ACCESS CONTROL	Response
1	Is an Access Control and policy and process in place requiring that access controls are in place to ensure that persons only have the minimal privileges they require on:	
2	All applications?	(Select One)
3	Operating systems?	
4	Databases?	(Select One)
5	Network devices?	
6	Is access to all systems and applications based on defined roles and responsibilities or job functions?	(Select One)
7	Are all user IDs uniquely associated with a specific individual?	
8	Is private data (such as SSN) prohibited from being used in User Ids to prevent revealing private user information?	(Select One)
9	Is level of access (e.g.: ADMIN) prohibited from being used in User Ids) to prevent revealing level of access?	
10	Is the sharing of user IDs prohibited?	(Select One)
11	Are the documents for granting access logged or archived?	
12	Are there formal processes in place to approve access to systems holding, processing, or transporting target data?	(Select One)
13	Are initial passwords communicated to users via a secure method?	
14	Are all new constituents issued random initial passwords?	(Select One)
15	Are users forced to change their password upon first logon?	
16	Are users forced to change their password on a pre-determined interval?	(Select One)
17	Are minimum password length controls in place and enforced?	
18	Is password composition of mixed characters enforced?	(Select One)
19	Is passwords history enforced and is it greater than 3?	
20	Is the length of time before failed login attempt count resets to zero greater than 24 hours?	(Select One)
21	Are all passwords encrypted:	
22	On sign-on display?	(Select One)
23	In transit?	
24	In storage?	(Select One)
25	Are there formal processes in place to regularly review access to ensure that only those people with a need-to-know currently have access?	
26	Are privileged user access rights reviewed on a periodic basis for appropriateness?	(Select One)
27	Are requirements in place specifying how long an inactive User ID can remain inactive before it is deleted or disabled?	
28	Is a policy in place to prohibit users from sharing passwords?	(Select One)
29	Are users required to lock their workstation before leaving it unattended?	
30	Are users required to terminate or secure active sessions when finished?	(Select One)
31	Is automatic screen saver/password re-verification on inactive on a workstation when left unattended for a predetermined time interval enforced?	
32	Is an automatic session termination enforced for users being inactive on an interactive server after a pre-determined time period?	(Select One)
33	Is a remote access solution present in the environment?	
34	VPN?	(Select One)
35	Are processes in place to ensure that connecting systems for supported hardware and software have:	
36	Current patch levels?	(Select One)
37	Current anti-virus?	
	Additional Information:	

Area 7	INCIDENT RESPONSE	Response
1	Does your company have a formal information security Incident Response Program / Plan in place?	
2	Is there a documented process in place to report suspected and actual security incidents?	(Select One)
3	In the event of an incident, is the incident response team available 24x7x365?	
4	Do your incident response processes address availability, confidentiality, and data integrity of your third party service providers?	(Select One)
5	Does your company have redundant/multiple communications connections to both primary and backup processing locations?	
6	Does the Incident Response Plan require the notification of customers in the event of an incident?	(Select One)
7	Does your incident response capability include forensic data collection and analysis techniques?	
8	Does your incident response capability include advance arrangements for third-party forensic and incident management services?	
	Additional Information:	

Area 8	BUSINESS CONTINUITY	Response
1	Is the Business Continuity and/or Disaster Recovery Policy / Plan tested at least annually?	(Select One)
2	Is your Business Continuity Plan and/or Disaster Recovery Policy/Plan periodically updated to address the rapidly changing threat landscape?	
3	Does your business continuity processes address both physical and cyber incidents?	
	Additional Information:	

Area 9	HOSTED WEB OR CLOUD APPLICATION	Response
1	Will the services provided to COSA include Data-as-a-Service (DaaS)? *Data is provided to COSA through specific interfaces.*	(Select One)
2	Will the services provided to COSA include Software-as-a-Service (SaaS)? *COSA uses your applications running on your cloud infrastructure.*	(Select One)
3	Will the services provided to COSA include Platform-as-a-Service (PaaS)? *COSA deploys onto your cloud infrastructure COSA-created or acquired applications created using programming languages, libraries, services, and tools supported by you.*	(Select One)
4	Will the services provided to COSA include Infrastructure-as-a-Service (IaaS)? *COSA is able to deploy and run arbitrary software, which can include operating systems and applications, on processing, storage, networks, and other fundamental computing resources you provide.*	(Select One)
5	Does the application support per-client security controls:	(Select One)
6	Password complexity requirements?	(Select One)
7	Password length requirements?	(Select One)
8	Password expiration?	(Select One)
9	Password history requirements?	(Select One)
10	Account lockout due to failed access attempts? (maximum of six)	(Select One)
11	Are passwords masked while entered?	(Select One)
12	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc.) for user access?	(Select One)
13	Can the application login screen be restricted to the COSA network IP range?	(Select One)
14	Does the application require transport encryption? (SSL)	(Select One)
15	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
16	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
17	Has the application been inspected for database injection attacks?	(Select One)
18	Have identified database injection vulnerabilities been remediated?	(Select One)
19	Has the application been inspected for session hijacking attacks?	(Select One)
20	Have identified session hijacking vulnerabilities been remediated?	(Select One)
21	Has the application been inspected for buffer overflow attacks?	(Select One)
22	Have identified buffer overflow vulnerabilities been remediated?	(Select One)
23	Does the application validate user input fields against malicious data entry?	(Select One)
24	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
25	Does the application restrict account administration through the website?	(Select One)
26	Does the application restrict system administration through the website?	(Select One)
27	Has the application been cleansed of built-in sample application code? (scripts)	(Select One)
28	Has the application been cleansed of built-in sample data?	(Select One)
29	Is application security assessed on a periodic basis?	(Select One)

Area 9	HOSTED WEB OR CLOUD APPLICATION	Response
30	Is the assessment performed by an external security consultant or company?	(Select One)
31	Is the assessment performed annually?	(Select One)
32	Is a security assessment performed after major upgrades to the application?	(Select One)
33	Are issues identified by a security assessment remediated ?	(Select One)
34	Do you have the ability to logically segment customer data so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	(Select One)
35	Can you provide the physical location of storage of a tenant's data upon request?	(Select One)
36	Do you allow tenants to define acceptable geographical locations for data routing or data storage?	(Select One)
37	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
38	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
39	Can you provide a documented procedure on how tenant data is sanitized from your systems once the service contract/relationship ends?	(Select One)
40	Do you "data mine" tenant data for your company's benefit?	(Select One)
41	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	

CITY OF SAN ANTONIO

Administrative Directive	**7.8d Access Control**
Procedural Guidelines	Controlling Access to City Systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	June 01, 2013
Revisions Date(s)	December 14, 2017
Review Date	
Owner	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides a framework for controlling access to the City of San Antonio's (COSA) information assets. It identifies requirements and responsibilities needed to properly manage access control, helping to ensure the confidentiality, integrity and availability of City system(s). This directive supersedes 7.8c on Remote Access, 7.8d on Account Access Management and 7.8e on User Account Management.

This directive is designed to help control logical and/or physical access to COSA information assets. COSA is subject to federal and state regulations and/or requirements that govern access control requirements (i.e. tax record laws/regulations, public records, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Criminal Justice Information Services (CJIS) policy for Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA), Payment Card Industry (PCI), etc.).

Controlling access to COSA systems prevents unauthorized access; limits access to sensitive resources; and restricts users to performing functions that are within the scope of their authority and/or responsibility. Access controls also assist in controlling the kinds of data, transactions, operations and activities that may be performed on COSA IT Systems. Appropriate access controls provide reasonable assurance and user accountability that access attempts, actions taken and transactions committed may be associated with a specific individual. Access Controls also pertain to the proper classification and protection of physical and logical diagrams, personnel listings, operations manuals, and IT system configuration information among other data. Improper access controls within units and departments can reduce the reliability and integrity of computerized data as well as increase the risk of data destruction, unauthorized program changes and/or other inappropriate disclosure of data. Should confidential information be disclosed, it could result in unnecessary vulnerabilities to the COSA environment.

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors, Partners and Other Third Parties

Definitions

Access	The ability to do something with a computer resource (use, change, or view).
Access controls	A manual or automated mechanism by which a system grants or revokes the right to access some data, or perform some action. Access controls are the means by which the access ability is explicitly enabled or restricted in some way and they enforce segregation of duties. Access controls can be onsite via local network, offsite via remote network and/or physical access by token or badge.
Authorization	The mechanism by which a system determines what level of access a particular authenticated user should have to sensitive resources or data controlled by the system.
Availability	The mechanism whereby systems and networks provide adequate capacity in order to perform in a predictable manner with an acceptable level of performance.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
Identification	The process whereby a network element recognizes a valid user's identity.
Information Systems	Computer(s), hardware, software, storage media, and network(s); the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
IT Resources	Any IT related or physical resource associated with IT such as IT infrastructure, databases, networks and software packages and applications.
Least Privilege	An access control principle requiring that a computer user be given only the level of access needed to perform their job duties.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Segregation of duties	The process of segregating work responsibilities to help ensure critical stages of a process is not under the control of a single individual.
User	Any employee or non-employee who uses COSA-administered information assets and/or system(s), exclusive of COSA's web pages.

Policy

- COSA is required to implement, access and apply security controls, including access control(s) to protect sensitive and regulated data by Federal and state laws/regulations, as well as industry standards (e.g. Payment Card Industry)
- The National Institute of Standards and Technology (NIST) Cyber Security Framework based on 800-53 Security Controls and industry best practices have been adopted by COSA to provide a protection framework for maintaining the confidentiality, integrity and availability of COSA systems and data.

- Organizational responsibility for the development, implementation, maintenance and/or compliance monitoring of this directive is placed with the Information Technology Services Department (ITSD).
- All information generated by and/or stored in COSA information technology systems are the property of COSA.
- Access to COSA's information and IT resources must conform to all administrative directives and ITSD security requirements.
- Access authorization should be formal, well-defined, documented and an auditable process.
- Access to COSA assets is based on an individual's membership in a group, job function and/or role in their assigned City department. Access permissions will use the principle of least privilege. All other access requires justification and approval.
- Logical and physical access controls implemented should be risk-based. Once access controls are implemented, they must be audited at least on an annual basis.
- A unique identifier and authenticator must be established for each individual (i.e., user ID) or process requesting access to COSA IT Systems.
- Where technically feasible and appropriate, access controls will enforce segregation of duties.
- COSA departments are responsible for non-employee and special account sponsorship and compliance with ITSD established provisioning and de-provisioning procedures.
- Remote access to COSA resources must comply with Human Resource (HR) and ITSD established provisioning and de-provisioning procedures.
- COSA Departments are responsible for ensuring compliance to this Directive.
- ITSD is responsible for monitoring compliance with this Directive.

This directive applies to:

- All information technology systems procured with COSA funds and/or used in the conduct of COSA business.
- All technology users who access COSA networks, data and/or applications including employees, contractors, consultants, vendors, partners and/or other third parties.
- All electronic messaging, equipment and technology that are owned or administered by the City including computers, mobile devices or personal devices reimbursed through COSA stipends (*A.D. 7.9*).
- All software, applications and/or, information system(s) developed by City personnel with City funds or licensed to the City.
- All data processed, stored and/or transmitted by a City Information Technology System(s).
- All data residing on 'Bring Your Own Devices' (BYOD) that use the COSA network.
- All remote access to the COSA network.
- All information collected or maintained by or on behalf of the City as well as all information assets used or operated by a City employee, a City contractor, a City vendor, or any other organization on behalf of the City.

Business Requirements for Access Control

- Users requesting physical access to a City facility controlled by an access control system or logical access to an information system must have completed the HR new employee or COSA third party sponsorship, background check, and attestation process.
- Local, physical and/or remote access to information resources must be explicitly approved through the user provisioning and de-provisioning, account access and/or the COSA ID request process.
- All access to the COSA network shall utilize ITSD approved technologies.
- Local, physical and/or remote access controls will be periodically reviewed for validity by ITSD, COSA department(s) and or application owners.

Non-Employee Access Requirements

To obtain local, physical and/or remote access to COSA IT resources, all third party non-employees (contractors, vendors, partners and consultants) must:

- Be sponsored by a City Department Business Owner through the non-employee provisioning process.
- Utilize defined user accounts that are only active during the individual's expected period of work or 90 days, whichever is shorter. Third party accounts not used for 90 days without prior notification will be disabled.
- The sponsoring Department is responsible for notifying Human Resources by submitting an SAP withdrawal/termination when a non-employee is no longer supporting their department.

User Access Management and Responsibility

- No individual shall engage in any activity which attempts to compromise COSA information assets or data regardless of intent.
- Any attempt to bypass or disable security controls or measures to gain unauthorized access to COSA IT assets or data is expressly forbidden.
- Departmental Data Owners are responsible for authorizing access to information.
- Access to COSA IT assets must be disabled upon separation of the employee.
- Accounts for individuals who are in a Leave of Absence (LOA) status must be disabled on the first date of absence and for the duration of the leave.
- All COSA Information Systems must be periodically screened for inactive accounts. Accounts will be disabled after 90 days of continuous inactivity or as soon thereafter as technically feasible.

Roles & Responsibilities

Employees	• Must follow the policy provided in this directive for all physical and logical access to COSA owned facilities, networks, systems and/or applications. • Must notify the ITSD Service Desk with any concerns regarding unauthorized physical or logical access to COSA owned facilities, networks, systems and/or applications.

Departments	• The Department Business System Owner is responsible for ensuring that appropriate access controls have been developed and documented in accordance with this AD. • Must Complete a COSA third party sponsorship process for any sponsored users. • Must notify HR and ITSD when a sponsored user is no longer providing support.
ITSD	• Maintains the user processes required for physical access and COSA domain user accounts. • Provisions and de-provisions access based on Departmental Business Owner authorization and approval. • Reviews and monitors data center access and domain user accounts. • Supports review process for Departmental physical and logical access controls. • Responsible for developing and maintaining an implementation standard and monitoring compliance for this directive for business systems under management control. • Responsible for working with HR to publish and disseminate the policies, standards and procedures which implement and enforce this directive.
Human Resources	• Provides support for the COSA third party sponsorship process for any sponsored users including provisioning or de-provisioning in SAP. • Support a periodic review of SAP third-party accounts that were suspended based on the ITSD 90-day inactivity review.

CITY OF SAN ANTONIO

Administrative Directive	**7.3a Data Security**
Procedural Guidelines	Regarding the use of Public and Confidential Data
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Revisions Date(s)	December 14, 2017
Last Review Date	August 3, 2018
Owner	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides guidance for compliance, confidentiality, privacy, security, and the associate governance for the City of San Antonio's (COSA) three data categories: (1) confidential, (2) agency-sensitive, and (3) Public. Data must be classified into one of these three categories when stored, processed, or transmitted on COSA resources or other resources where COSA business occurs. This AD establishes and identifies responsibility for such data and provides a framework for maintaining compliance with applicable laws, regulations, and standards. Security standards, which define these security controls, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

Policy

This directive establishes guidance for developing, maintaining, publishing, and administering comprehensive data governance and information technology system security. This directive references applicable local, state, and federal law.

Departmental data owners are responsible for the classification and protection of data under this directive. Precautions shall be taken to reasonably assure the confidentiality, integrity and availability of the protected data. Access to protected data shall be based on legitimate business need. COSA data shall be disseminated in accordance with this directive.

This directive applies to:

- All data processed, stored and/or transmitted by a COSA Information Technology System(s)
- All COSA data processed, stored and/or transmitted on personally-owned devices also referred to as "Bring Your Own Device" (BYOD)
- All data collected or maintained by or on behalf of COSA in any form (electronic or hardcopy).

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees

☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	

Definitions

Bring Your Own Device (BYOD)	The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.
City-administered information technology system(s)	Any technology or equipment that is used and/or managed by COSA even if COSA does not own the technology or equipment. COSA-managed information technology system(s) includes technology or equipment owned by COSA, on loan to COSA, funded by grants, leased by COSA.
Criminal Justice Information Services (CJIS) Security Policy	CJIS Security Policy represents the shared responsibility between Federal Bureau of Investigation CJIS and the CJIS Systems Agency and State Identification Bureaus.
Data Owner	The data originator or entity that can authorize or deny access to the data. The data owner has the ability to create, edit, modify, share and determine access restrictions to the data they control. They are responsible for the accuracy and integrity of the data they own.
Local Statutes	The ordinances, statutes, and laws of COSA, Bexar County and/or the municipality or county where the user is located.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record.
Network	A group of two or more computers linked together to facilitate communication, data sharing, and processing among other computer-based activities.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
Records Management Officer	The person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction.
Sensitive PII	Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
State Statutes	The statutes and laws of the state of Texas and/or the state where the user is located. Where statutes from two states conflict, the statutes of Texas and federal government shall take precedence.

Policy Guidelines

Adherence to this directive will help reasonably assure the confidentiality, integrity, and availability of COSA data:

- COSA has adopted the National Institute of Standards and Technology (NIST) 800-53a Security and Privacy Controls to provide a data protection framework for maintaining the confidentiality, integrity and availability of data.

- Baseline security controls for COSA Information Systems shall be based on the data owner's data classification as governed by this directive
- COSA data shall be classified as public, agency- sensitive, or confidential

Data Classification and Open Records

All data shall be classified as public, agency – sensitive, or confidential for the purpose of establishing dissemination guidelines and protective security measures. AD 1.31 Open Records (Texas Public Information Act) places responsibility for developing and updating the Municipal Open Records Policy with the City Attorney's Office. This requirement includes any response to open record Request (ORR) whether or not the records are public under the Open Records/Texas Public Information Act of 1993. All open records shall be reviewed by the department data owners prior to dissemination to reasonably assure that open records do not contain confidential data or sensitive Personally Identifiable Information (PII).

Confidential Data

Confidential data requires the highest level of protection. Accidental or intentional disclosure of this type of sensitive data could cause damage and/or serious harm to COSA and/or its citizens.

Confidential data may not be freely disseminated. This type of data is generally restricted from disclosure by local, state and federal statues, ordinances, directives and/or court orders.

Examples of "confidential" data may include but are not limited to: Sensitive PII (such as name in combination with Social Security Number (SSN))

Sensitive PII is any combination of information or data that permits the identity of an individual to be directly or indirectly inferred, traceable, linked and/or linkable to a specific individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, or visitor to the U.S. In addition, sensitive PII combinations if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, and/or unfairness to an individual.

Below is a list of data that is always Sensitive PII:

- Social Security Numbers
- Alien Registration Numbers (A-numbers)
- Passport Numbers
- Driver's license Numbers or state identification numbers
- Biometric Identifiers (fingerprint, iris scan, voice print)
- Genetic Data network
- Physically secure hardcopy protected data in a locked drawer, file cabinet, desk and/or safe.

The following information is classified as Sensitive PII when linked with the person's name or other unique identifier, such as an address or phone number:

- Citizenship or Immigration status
- Criminal History
- Medical Information
- Bank Account or Routing/Transit Numbers
- Credit Card Numbers.
- Income Tax Records
- Full Date of Birth
- Financial or Bank Account Numbers
- Fingerprint Identification Number (FIN) or Student and Exchange

Agency- Sensitive
This is sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of "Agency-Sensitive" data may include but are not limited to:

- COSA operational information
- COSA personnel records
- COSA information security configurations, data, and procedures
- Vendor bids and/or contract cost estimates among other sensitive data types

Public
Public data is all data and information not classified as confidential or agency-sensitive.
The data owner, or designated employee of the data owner, may disseminate and disclose the data or information derived from the data to anyone upon request. ORR fees have been established for extracting and delivering this type of data.

Protection of Confidential Data & Personally Identifiable Information

1. **All Departmental Data Owners must:**
   - Implement cost effective internal controls, safeguards and/or countermeasures to protect data. All preventative, detective and/or corrective controls shall be risk based. The cost of all management, operational and/or technical controls shall be commensurate with the value of the data.
   - Preserve citizen privacy and respect individuals choice to consent when collecting, using, sharing, and/or disclosing of customer, partner, or employee personal information.
   - Limit the use and storage of confidential data and sensitive PII to what is only necessary.
   - Determine encryption requirements based on regulatory requirements.
   - Not store confidential and/or sensitive data longer than is absolutely necessary.
   - Only collect data when COSA has the legal authority to do so, and if required have a Privacy Act System of Records Notice (SORN) in place that describes the information.
   - Minimize the distribution and proliferation of protected data.
   - Keep protected data relevant, accurate, timely and not excessive in relation to the purpose such data is processed, stored and/or transmitted.
   - Establish departmental procedures for dissemination of protected data in compliance with AD 1.31 and Open Records as well as establish and enforce departmental procedures and protections in addition to this Directive to reasonably assure the security of the specific data owned.
   - Periodically review data protection procedures, controls, and safeguards to reasonably assure that internal controls, countermeasures and/or safeguards are working as intended.

2. **COSA Information Systems must:**
   - Use security controls to protect against unauthorized access, disclosure, modification and destruction to reasonably assure the confidentiality, integrity, availability of data.
   - Follow NIST encryption and security protocol standards for protected data as required.

3. **Employee and Third Parties must:**
   - Safeguard COSA's data resources and comply with the provisions of relevant COSA Security ADs
   - Comply with all COSA procedures regarding protected data.
   - Receive written approval from both his/her department director to store sensitive data.
   - Report suspected violations to supervisor or manager, department head, and the Chief Information Security Officer (CISO) as well as the HIPAA Privacy Officer if healthcare data.
   - Only store protected data on COSA owned device(s).
   - Ensure personal devices are not used to store, process and/or transmit unencrypted protected data.
   - Ensure unencrypted confidential data and sensitive PII is not transmitted outside of COSA.

Data Laws and Standards

Regulation and industry standards that protect confidential and sensitive data include, but are not limited to:

- The U.S. Privacy Act of 1974 (5 U.S.C.A. 552a)
- U.S. Electronic Communications Privacy Act of 1986 (ECPA)
- The Open Records/ Texas Public Information Act of 1993 (TPIA)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Texas Business and Commerce Act, Section 521.053
- Texas Identity Theft Enforcement and Protection Act of 2007 (ITEPA)
- Texas Medical Privacy Act of 2001 (TMPA)
- Payment Card Industry Security Standards (PCI)
- Criminal Justice Information Services Security Policy (CJIS)

Data Destruction

Electronic records shall be destroyed in accordance with Section 441.185 Government Code and COSA record retention policies. All data storage device(s) and/or information system(s) containing protected data shall be sanitized or the storage device destroyed. COSA shall arrange for destruction of protected data by shredding, degaussing, erasing and/or otherwise modifying the sensitive data in the records to make the information unreadable or indecipherable. Additional information on sanitization tools and methods of destruction based on Department of Defense 5220.22-M data destruction standards (available at http://www.dir.state.tx.us). Documentation shall also be maintained that documents the data, description of device, data destruction process and sanitization tools used to remove or destroy data.

Roles & Responsibilities

Employees	Adhering to all guidance provided in this directive.
Departments	COSA departmental data owners are responsible for data classification and identification of data protection requirements.
ITSD	COSA Information Technology Services Department (ITSD) is responsible for publishing, disseminating, and maintaining this directive.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8888.

City of San Antonio – Aviation Department

Request for Competitive Sealed Proposals – Rideshare Monitoring Services for San Antonio International Airport (RFCSP 22-079, RFx 6100015294)

Friday, August 26, 2022, 2:00 p.m. Central Time
At San Antonio International Airport, Terminal A Mezzanine Conference Room
Prospective Respondents may also join via conference call using the following instructions:
Dial-In Number: 1-415-655-0001
Access Code: 2453 470 8622
or
via WebEx at www.webex.com and clicking on join.
The meeting number is 2453 470 8622 and password is COSA

PLEASE HOLD ALL QUESTIONS UNTIL THE END OF THE PRE-SUBMITTAL CONFERENCE

I. **Welcome and Introductions**
City of San Antonio SAePS Portal –
https://supplierservice.sanantonio.gov/irj/portal

II. **Overview of Background and Scope of Services**

III. **Term of Contract**

IV. **Overview of RFCSP Process:**

- **A. RFCSP Requirements**
- **B. Submission Instructions**
- **C. Restriction on Communications**
- **D. Evaluation Criteria**

V. **Key Points/Reminders:**

A. Restrictions on Communication
Please refer to RFCSP Section 003 – Instructions to Respondents for contact information and protocol. **Final Questions Accepted: 10 calendar days prior to the date proposals are due.**

All written questions are to be sent to:
Marisol Amador, Procurement Specialist III
City of San Antonio, Aviation Department – Purchasing Division
marisol.amador@sanantonio.gov

B. Following is a list of **projected dates/times** with respect to this RFCSP:

RFCSP Release Date	August 17, 2022
Pre-Submittal Conference	August 26, 2022 @ 2:00 p.m. CT
Final Questions Accepted	September 9, 2022
Proposals Due	**September 19, 2022 @ 2:00 p.m. CT**

C. Proposal Submission:

Proposals will only be accepted electronically

Electronically through SAePS Portal- https://supplierservice.sanantonio.gov/irj/portal

LATE PROPOSALS WILL NOT BE ACCEPTED.

D. Further Information:
Changes to the RFCSP and responses to questions may be posted to the City of San Antonio's SAePS portal, **– https://supplierservice.sanantonio.gov/irj/portal.** It is Respondent's responsibility to review this site and ascertain whether amendments or revisions have been made prior to submission of a proposal. No oral statement of any person shall modify or otherwise change, or affect the terms, conditions, or specifications stated in RFCSP. Changes, if any, to the RFCSP shall be made in writing only.

E. Vendor Guide to Solicitation Response:
http://www.sanantonio.gov/Portals/0/Files/Purchasing/pdf/vendor-RFx-training-guide.pdf
If you need immediate assistance viewing a solicitation or submitting a response, call the Vendor Support Line at 210-207-0118 or e-mail **vendors@sanantonio.gov**.
Please indicate the name and number of the solicitation in the e-mail subject line. (Please allow 1-2 working days for them to response)

VI. Questions

VII. Adjourn

ADDENDUM I

SUBJECT: Request for Competitive Sealed Proposal, Rideshare Monitoring Services for San Antonio International Airport, (**RFCSP 22-079; 6100015294**), Scheduled to Open: September 19, 2022. Date of Issue: August 17, 2022.

FROM: Jennifer Johnson
Procurement Administrator

DATE: September 15, 2022

THIS NOTICE SHALL SERVE AS ADDENDUM NO. I TO THE ABOVE REFERENCED REQUEST FOR COMPETITIVE SEALED PROPOSALS

THE ABOVE-MENTIONED REQUEST FOR COMPETITIVE SEALED PROPOSALS IS HEREBY AMENDED AS FOLLOWS:

1. **Change:** Proposal deadline is hereby extended to 2:00pm Central Time, on September 23, 2022.

2. RFCSP Section 003-Instructions for Respondents, Part B, Submission Requirements, is hereby revised to add the following:

   THIRD PARTY VENDOR IT CLOUD SECURITY QUESTIONNAIRE. If a Software as a Service (SaaS) solution is proposed, the respondent will be required to complete the appropriate Third-Party Vendor IT Cloud Security Questionnaire provided under Attachment G.

3. Pre-Submittal Conference Sign-In Sheet is hereby added as RFCSP Attachment L and posted as a separate document.

4. RFCSP Attachment K, Proposal Checklist, is hereby deleted and replaced with RFCSP Attachment K – Proposal Checklist Revision I.

QUESTIONS SUBMITTED IN ACCORDANCE WITH RFCSP SECTION 003, INSTRUCTIONS FOR RESPONDENTS:

On August 26, 2022, the City of San Antonio hosted a Pre-Submittal Conference to provide information and clarification for the Rideshare Monitoring System Request for Competitive Sealed Proposals. Below is a list of

questions that were asked at the pre-submittal conference. The City's official response to questions asked is as follows:

Question 1: Apart from what is stated in the RFCSP, are there any challenges or workflow problems with the current system that the City is looking to resolve?
Response: No.

Question 2: What is the anticipated date for contract award?
Response: December 2022.

Question 3: What is the City's budget for this contract?
Response: The City is not providing this information at this time.

Jennifer Johnson

Jennifer Johnson
Procurement Administrator
Finance Department – Purchasing Division

City of San Antonio Aviation Department
Rideshare Monitoring Services RFCSP 6100015294; 22-079

Pre-Submittal Conference Sign-in Sheet

Date: August 26, 2022 **Time: 2:00 p.m.Central Time**

NAME (Print Legibly)	COMPANY	EMAIL ADDRESS	PHONE NUMBER
Marisol Amador	City of San Antonio	marisol.amador@sanantonio.gov	210-207-3406
Procurement Specialist III	Finance/Aviation Department		
Tamera Irwin	City of San Antonio	tamera.irwin@sanantonio.gov	210-207-3467
Airport Parking Manager	Aviation Department		
Lynn Richardson	GateKeeper	ldr@gksys.com	651-365-0700 (Phone)
			651-365-0777 (Fax)
Brian Richardson	GateKeeper	brichardson@gksys.com	651-365-0700 (Phone)
			651-365-0777 (Fax)
Jessica Davis	Lacuna Technologies		

You are not required to provide your address, phone number or email address; however, doing so makes it easier to contact you regarding this solicitation if you have not yet registered in SAePS.

ALL INFORMATION PROVIDED BY YOU ON THIS FORM MAY BE POSTED ON THE CITY'S WEBSITE, OR OTHERWISE DISSEMINATED PUBLICLY. BY INCLUDING THE INFORMATION, YOU HEREBY AFFIRMATIVELY CONSENT TO THE RELEASE OF THE INFORMATION YOU PROVIDE.

007 - SIGNATURE PAGE

By submitting a proposal, Respondent represents that:

(s)he is authorized to bind Respondent to fully comply with the terms and conditions of City's Request for Competitive Sealed Proposals for the prices stated therein;

(s)he has read the entire document, including the final version issued by City, and agreed to the terms therein;

Respondent is in good standing with the Texas State Comptroller's Office; and

to the best of his/her knowledge, all information is true and correct.

Complete the following and sign on the signature line below. Failure to sign and submit this Signature Page will result in rejection of your proposal.

Respondent Information
Please Print or Type

Vendor ID No.	41-1887879
Signer's Name	Brian Richardson
Name of Business	GateKeeper Systems, Inc.
Street Address	1875 Plaza Drive, Suite 200
City, State, Zip Code	Eagan, MN 55122
Email Address	brichardson@gksys.com
Telephone No.	651-365-0700
Fax No.	651-365-0777
City's Solicitation No.	6100015294; 2022-079

Brian Richardson
Signature of Person Authorized to Sign Proposal

RFCSP ATTACHMENT B - PRICE SCHEDULE

RFCSP 22-079, 6100015294, Rideshare Monitoring Services for San Antonio International Airport

06

Respondent Name:

Provide the following information regarding Respondent's software
and submit with your proposal the appropriate Attachments G if a SaaS solution is proposed.

Software is Off-Premise Vendor Hosted:	☑ Yes	or	☐	No
Software is On-Premise City Hosted:	☐ Yes	or	☑	No

Item	Initial Period	Year 2	Year 3	Year 4	Year 5	Total Cost
1. What is the TOTAL, all-inclusive - System Application - cost for ALL software being proposed in the proposed system?						
1A System Application						
One-time License Fee with 1 Year Warranty	N/A					0
Recurring license fee	$ 14,000.00	$ 14,600.00	$ 15,200.00	$ 15,900.00	$ 16,600.00	$ 76,300.00
Annual Maintenance Fee	N/A					0
One-Time Setup Fee	N/A					0
Hosting / Service Cost	$ 2,000.00	$ 2,100.00	$ 2,200.00	$ 2,300.00	$ 2,400.00	$ 11,000.00
1B Other Software - One-time License Fee						
Database	N/A					0
Software	N/A					0
Operating System and Utilities	N/A					0
Development Tools	N/A					0
Reporting Tools	N/A					0
Other Software - One Time Fee	N/A					0
1C Other Software - Re-Occurring Maintenance/Support Fee						
Database	N/A					0
Software	N/A					0
Operating System and Utilities	N/A					0
Development Tools	N/A					0
Reporting Tools	N/A					0
Other Software - One Time Fee	N/A					0
2. What is the TOTAL, all-inclusive - Specialized Hardware - cost for ALL software being proposed in the proposed system?						
2A Specialized Hardware - One Time Cost						
(vendor to provide list and costs)	N/A					0
	N/A					0
	N/A					0
	N/A					0
2B Specialized Hardware - Re-Occurring Maintenance/Support						
(vendor to provide list and costs)	N/A					0
	N/A					0
	N/A					0
3. What is the TOTAL, all-inclusive - Solution Implementation cost for ALL software being proposed in the proposed system?						
3a. Project Initiation and Management	N/A					0
3b. Functional Requirements/Validation	N/A					0
3c. Software Installation	N/A					0
3d. System Design	N/A					0
3e. System Configuration	N/A					0
3f. Development- Customization	N/A					0
3g. Development-Integration	N/A					0
3h. Development - Other	N/A					0
3i. Conversion/Migration	N/A					0
3j. System Testing	N/A					0
3k. Training Deployment	N/A					0
3l. Cut-Over, Go-Live, Post Go Live	N/A					0
3m. Final Acceptance Testing	N/A					0
3n. Other-Implementation	N/A					0
4. What is the TOTAL, all-inclusive - Other Costs for ALL software being proposed in the proposed system?						
(vendor to provide list and costs)	N/A					
						0
						0
Total Fixed Cost	$ 16,000.00					$ 16,000.00
Total Recurring Costs		$ 16,700.00	$ 17,400.00	$ 18,200.00	$ 19,000.00	$ 71,300.00
Total system cost						**$ 87,300.00**