TUCSON AIRPORT AUTHORITY
INFORMAL REQUEST FOR PROPOSALS FOR

TERMINAL AUTOMATED TELLER MACHINES

Responses to this RFP must be submitted by 2:00 p.m. LOCAL TUCSON TIME on Monday August 19, 2024. **Proposals received after 2:00 p.m. local Tucson time will not be considered.** Proposals must be emailed to dcruz@flytucson.com or delivered to: Tucson Airport Authority, Tucson International Airport, 7250 S. Tucson Blvd., Suite 300, Tucson, AZ 85756. Attn: Debbie Cruz.

All questions regarding this RFP should be submitted **in writing** no later than 5:00 p.m. local Tucson time on Friday, July 19, 2024. All instructions regarding the RFP shall be in writing. TAA shall not be responsible for any oral instructions. For more information or an alternate format of this RFP, please contact Debbie Cruz at 520-573-4831 or dcruz@flytucson.com. The proposal must be complete and include all of the information requested in this RFP.

Request for Proposals (RFP)

I. INTRODUCTION AND GENERAL DESCRIPTION

A. For the convenience of the traveling public, the Tucson Airport Authority (TAA) is seeking proposals from qualified operators to add automated teller machines (ATMs) at Tucson International Airport (TUS or Airport) on a non-exclusive basis. The contract(s) are anticipated to commence on a date determined after the selection process.

The Airport consists of a main terminal complex, two concourses (Concourses A and B). TUS is currently served by six airlines including Alaska, American, Delta, Southwest, Sun Country and United. In CY2023, TUS hosted approx. 3.8 million passengers, 10% increase from CY2022. Additional passenger statistics information is available via the following link: https://www.flytucson.com/taa/media-center/statistics/.

B. Business Terms

1. Contract. A draft Agreement is provided as **EXHIBIT A. Proposer is advised to read the draft contract carefully. The overview included in this RFP is not intended to detail all obligations outlined in the Agreement.** NOTE: TAA reserves the right to revise the draft contract prior to its execution.

2. Term. The Operating Term will commence on a date determined upon completion of the selection and extend three (3) years with two one-year renewal options to be exercised in the sole discretion of TAA.

3. **Locations**. Pre-Security ATMs will be located on the 1st floor baggage claim area of the terminal near the welcome lounge for B Concourse and 2nd floor behind the Arroyo Trading Post. Both locations are indicated on the attached **Exhibit B** and may be accessed from the non-secure area of the terminal**.** Post-security ATMs will be located on A Concourse and B Concourse on the 2nd floor in between the concessions area and departure gate areas. Both locations are indicated on the attached **Exhibit B** and may only be accessed from the secure area of the terminal. TAA reserves the right, in its sole and absolute discretion, to position the ATMs in locations in the terminal as it deems appropriate or necessary.

4. Non-Exclusive Agreement. TAA shall enter into a non-exclusive agreement with one or more successful proposer(s) for the ATM locations.

II. PROPOSAL INSTRUCTIONS AND REQUIREMENTS

A. Proposal Requirements. To expedite the evaluation of proposals, each proposer must organize its proposal as outlined in this RFP. Proposals should be prepared simply and economically, providing a straightforward, concise description of the proposal to meet the requirements of this RFP. TAA may deem any proposals that do not follow the format specified below as non-responsive and disqualify them from further consideration. In addition, failure on the part of the proposer to provide the required documentation may be cause for rejection of the proposer's proposal. TAA shall have the sole discretion to resolve any conflict between or among any of the proposal forms. All proposals must include the following information in this order:

- Provide a brief overview of the company including the number of ATMs currently operated by the company and a general summary of their placement locations.

- Describe the type of machine proposed and include a photo, rendering, or other depiction of the machine. The proposed ATM must have a system management capable of predicting, assisting, and reporting maintenance and the need for cash replenishment.

- Provide the proposed amount of fee to be charged to users of the ATM ("Transaction Fee").

- Proposed percentage of Transaction Fee to be paid to TAA ("Privilege Fee").

- Describe the minimum and maximum amount of withdrawal supported by the ATM.

- Describe the networks, credit cards, and/or banks supported by the ATM.

- Describe the languages supported by the ATM; at a minimum, all ATMs should support English and Spanish language.

- Describe the maintenance and cleaning schedule for the ATM, including response time for emergency or after-hours response.

- Describe the protocol to ensure the security of individuals using the ATM.

III. SELECTION Of PROPOSER AND AWARD OF AGREEMENT

A. Basis for Contract Award

A Selection Committee will evaluate each proposal. Proposers will be ranked based upon the overall quality of the Proposal. TAA will select the proposer(s) who in TAA's sole judgment are determined to be the best-qualified and responsible proposer(s) and whose proposal, in TAA's sole judgment, are deemed the most desirable and advantageous to TAA and the traveling public. In no case will an award be made until the financial responsibility, operational ability, insurance sufficiency, and standards of the successful Proposer have been investigated and found by TAA, in TAA's sole discretion, to provide adequate assurance of the Proposers ability to fulfill the terms of the Agreement. TAA reserves the right to waive any formality or irregularity in any proposal, letter of credit or surety bond, to reject any or all proposals or to negotiate for the modification of any proposal with its proposer.

Time of Award

It is the intent of TAA to make an award or rejection of Proposals within thirty (30) days following the receipt of Proposals, or as soon as reasonably practicable thereafter.

B. Rejection or Acceptance of Proposals

The requirements of this proposal package are for the benefit and protection of TAA; therefore, the right is reserved by TAA to waive any irregularities in the completion of the forms enclosed in this RFP; to accept or reject any or all proposals; and to readvertise for proposals which will provide the best service to TAA. Any form submitted which is incomplete, conditional, obscure, or which contains additions not called for, or irregularities of any kind, may be cause for rejection of the proposal.

EXHIBIT A - DRAFT AGREEMENT

TUCSON AIRPORT AUTHORITY

CONCESSION AGREEMENT

This Concession Agreement ("Agreement") is entered into this ____ day of _____ 2024, (the "Effective Date"), by and between the Tucson Airport Authority, an Arizona nonprofit corporation ("TAA"), and _____, ("Operator"), collectively referred to as the "Parties".

RECITALS

The Parties acknowledge that the following recitals are true and correct and constitute an integral part of this Agreement.

A. TAA operates and manages the Tucson International Airport located at 7250 S. Tucson Blvd., Tucson, AZ 85756 ("Airport") in accordance with a lease with the City of Tucson pursuant to which TAA is authorized to enter into this Agreement.

B. Operator is the owner of certain Automated Telling Machine ("ATM") systems whereby ATMs are available on self-service basis to the public.

C. Operator seeks permission from TAA to enter the Airport to provide Services for the public.

D. The parties have agreed upon the installation and operation of ____ self-service ATMs in the terminal building at the Airport, upon the terms and conditions stated in this Agreement.

NOW THEREFORE, in consideration of the foregoing recitals, and for other good and valuable consideration subject to the following conditions and for the purposes hereinafter contained, the parties mutually agree as follows:

AGREEMENT

1. Use. TAA hereby grants to Operator an Agreement, under the terms and conditions set forth herein, for Operator to enter the Airport to provide Services for the public. ATM's will be in the locations as shown on Exhibit A and may be relocated by Operator from time to time as approved or directed by TAA. Operator shall not change locations of ATM's ("Premises") without TAA's prior written approval.

2. Term & Termination. The term of this Agreement shall begin on the Effective Date above and end on _____, 20___. Operator shall have the right to request an extension of the Term of this Agreement for two (2) additional one-year periods ("Extension Term"). Such right may be exercised by giving TAA written notice (in accordance with Section 13 of the desire to extend the Term no later than 90 days prior to the expiration of the Initial Term and may be granted by the TAA (a) at TAA's sole discretion and (b) conditioned upon Operator's material compliance, at all times during the Term, with all of its duties and obligations under the Agreement. TAA may

terminate this Agreement at any time and at its sole and absolute discretion, upon ten (10) days written notice of such termination to Operator, or immediately upon written notice in the case of safety or security violations by Operator at the Airport.

3. Obligations of Operator.

a. Operator shall provide not less than two (2) ATM's. Operator shall service and upgrade the ATMs as reasonably directed by TAA and agreed to by the Operator to meet the needs of the public.

b. A product/equipment specification sheet, including communications protocol utilized to communicate between ATM's, along with detail logic diagram and other technical information and documentation as requested by TAA, at its sole discretion, are required for review and written approval by TAA prior to installation.

c. Operator is responsible for furnishing all equipment and materials, management, labor, and trained personnel, which may be necessary to install, and service ATMs at its sole cost and expense. Once installed, Operator may not remove or alter any equipment without the prior written consent of TAA which consent TAA may withhold at its reasonable discretion.

d. The ATMs shall be in in operation twenty-four hours a day, every day, year around. Should an ATM become inoperable, it shall be serviced, repaired or replaced within twenty-four hours.

e. Operator shall designate a local representative for the ATMs in the Airport. Operator shall provide TAA with the current name, address, and telephone number of its local representative. Operator's local representative shall respond to the Airport premises upon written or oral request by TAA within twenty-four (24) hours and promptly resolve any issues regarding the ATM's operations at the Airport.

f. Not later than ten (10) days after expiration or termination of this Agreement, Operator shall remove any and all personal property and equipment from the Airport. Upon failure of Operator to remove such personal property within such ten (10) day period, title thereto shall vest in TAA and TAA shall have the right and option to remove the same, restore the Airport, and receive from the Operator the cost and expense of doing so.

4. Operations, Fee, and Billing. Operator shall pay _____ to TAA during the Term of this Agreement. Operator is also responsible for all other applicable fees and costs associated with its operations at the Airport, including, but not limited to, badging fees, and parking fees. Operator acknowledges and agrees that the Airport rates and fees may be amended at any time by TAA in TAA's sole discretion.

a. Taxes. Operator shall pay any sales tax, transaction privilege tax, or other exaction assessed or assessable as the result of its conduct of business at the Airport under authority of this

Agreement including any such tax payable by TAA.

b. Activity Report. Operator shall, no later than ten (10) calendar days after each month's end, send to TAA, via electronic means, a report detailing number of transactions, fees collected by Operator, deposit amounts and other data as requested by TAA for the preceding quarter.

c. Interest/Administrative Charge. Payments not received when due shall accrue interest from the due date at the rate of one- and one-half percent (1.5%) per month. In addition, if any payment due hereunder is more than ten (10) days past due, Operator shall pay TAA an amount equal to five percent (5%) of such payment as an administrative charge to offset the administrative burden created by late payments.

5. No Lien; No Exclusive Right. This Agreement is not intended to be and shall not become an encumbrance, charge or lien on the Airport and property owned by TAA. It is understood that nothing herein contained shall be construed to grant or authorize the granting of an exclusive right within the meaning of 49 U.S.C. § 40103(e).

6. Privilege Fee. As consideration for TAA authorizing the Operator to conduct a non-exclusive ATM service concession at the Airport, Operator shall pay to TAA a fee of $_____ per withdrawal transaction.

7. Payment Due Date. The Privilege Fee shall be paid monthly for the preceding month's business. Privilege Fees are due and payable without further notice or demand, no later than the twentieth (20^{th}) day of each month for the preceding month. If any payments are not received by TAA on or before the due date each month, Operator shall pay an interest fee of one percent (1%) per month (12% annually) for each month or partial month that any payment due is not made.

8. Place of Payment. Operator shall make all payment of fees and other charges to the TAA at its administrative offices or at such other place as may be designated by TAA from time to time.

9. Advertising and soliciting. Operator may not conduct advertising on the Airport without the prior written approval of TAA and only through the TAA's approved Airport advertising concessionaire(s).

10. Compliance with Laws, Rules, and Regulations.

a. General. Operator shall comply with all applicable local, state, and federal laws, ordinances, statutes, rules, regulations, procedures, and orders, including but not limited to those of the of the U.S. Department of Transportation, the State of Arizona, Pima County, the City of Tucson, and all agencies thereof now in effect or hereafter promulgated; and further, Operator will display to TAA any permits, Agreements or other evidence of compliance with such laws upon request.

b. Nondiscrimination. Operator does hereby covenant and agree that no person on

the grounds of, race, color, or national origin shall be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination (i) in the use of said Services, or (ii) under contract to provide Services to Airlines, or (iii) as an employee, contractor, or subcontractor of Operator. Further, Operator shall use the Premises in compliance with all other requirements imposed by or pursuant to Title 49, Code of Federal Regulations, DOT Subtitle A, Office of the Secretary, Part 21, Nondiscrimination in Federally Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Act of 1964, and as said Regulations may be amended. Each person exercising any rights hereunder shall comply with all such laws. A violation of any such laws by Operator, its agents, employees, customers, patrons, guests, or any other person claiming rights hereunder shall constitute material breach of this Agreement and TAA shall have the right to terminate this Agreement immediately, without notice.

c. Public Records. Operator acknowledges and agrees that TAA complies with the Arizona Public Records Laws, and all information Operator provides to TAA is subject to disclosure pursuant to the provisions of Arizona Public Records Laws. Operator agrees that this Agreement does not require Operator to submit any confidential business information or trade secrets toTAA.

d. Prohibited Activities. Operator, and Operator's officers, directors, agents, contractors, Operators, or employees shall not engage in any business activity or commercial operation at Tucson International Airport other than that permitted by this Agreement without a written Agreement with the TAA.

11. Insurance. Prior to conducting its service operation at the Airport, Operator, for itself and its officers, representatives, agents, employees, contractors, subcontractors, Operators, invitees and suppliers shall comply with all applicable insurance requirements as set forth in Exhibit C. Insurance coverage must include all of Operators authorized vehicles and drivers, premises and operations of Operator and must be in full force and effect throughout the term of this Agreement.

12. Indemnity. Operator shall indemnify, defend and hold harmless TAA, and the City of Tucson, and all TAA and City of Tucson officials, directors, officers, employees and authorized agents, for, from and against any and all losses, costs (including attorney fees), damages, expenses and liabilities ("Losses") arising out of any third party claims arising from the activities of Operator or its officers, directors, agents, contractors, Operators, or employees at the Airport pursuant to this Agreement or in connection with any and all claims for damages as a result or an injury or death of any person or persons or damages to any property which arises as a result of any act or neglect on the part of Operator or its officers, directors, agents, contractors, Operators or employees related to Service provided under this Agreement.

13. Notice of Claims, Defense, Survival of Obligations. The parties shall give each other prompt notice of any claim made or suit instituted which in any way directly or indirectly affects or might affect the right of the parties hereto, and each party shall have the right to compromise and defend the same to the extent of its own interest. Operator shall have sole control over the defense and settlement of any claims subject to indemnification pursuant to Section 7 and TAA shall provide reasonable cooperation in such defense. Operator's settlement of any claim pursuant to this authority in no way limits Operator's indemnification requirements under Section 7. TAA shall have

the right, but not the duty, to participate (at its own expense) in the defense of any claim with attorneys of TAA's selection without relieving Operator of any obligations hereunder. Operator's obligation hereunder shall survive any termination of this Agreement or Operator's service or activities on the Airport.

14. Assignment. Operator shall not assign or transfer any portion of its interest under this Agreement, nor permit any other person, firm, or corporation to perform the Service on its behalf without the prior written consent of TAA, which consent may not be unreasonably withheld.

15. Compliance with Federal Regulatory Requirements and Security Measures Implemented by TSA:

a. Operator agrees to comply with Federal Aviation Regulations and Transportation Security Administration ("TSA") regulations related to aviation security under 49 CFR Part 1542 and 1540. Operator further agrees that any charges, fees, or fines levied upon and paid by TAA through enforcement of Federal Aviation regulations, Transportation Security Administration regulations or any subsequent regulation due to acts by Operator's employees, agents, suppliers, contractors, guests, or patrons shall be borne by Operator. TSA, TAA or its agents, employees, and representatives may at any time inspect Operator's authorized vehicles for purposes of monitoring compliance with this Agreement and Federal Regulations, as may be updated from time to time, while such vehicles are on Airport premises, and Operator shall notify its authorized drivers and employees of this requirement. As Operator's activities will take place at the secured sections of the Airport, Operator is required to ensure that all its employees obtain photo identification badges which include fingerprinting process and applications being submitted through the TAA Airport Security Office ("ASO") to obtain a Security Identification and Display (SIDA) badge ("SIDA Badge") prior to operating at the Airport. If any Operator's SIDA Badge is lost, stolen or damaged, the cost of a replacement badge is the responsibility of the employer. The Operator employees are required return their SIDA Badge to ASO immediately after his/her termination of employment at the Airport. All persons obtaining a SIDA ID badge will comply with all rules, regulations, guidelines, and policies concerning airport security and use of the badge. A ten-year verifiable background check is also required. Violation of the rules and regulations set forth by the TSA, as well as access to an unauthorized area without a badge, may result in sizable civil penalties. Operators and their employees must wear badges visibly on their outer garments, above their waists at all times. TAA personnel may suspend and/or confiscate the badge of any employee who is not displaying his/her badge as required. Badge may only be used by the individual to whom it is issued.

b. Operator understands and agrees that in the event the TSA assesses a civil penalty or fine against TAA for any violation of Transportation Security Regulation or other federal statute as a result of any act or failure on the part of Operator (including its employees, subcontractors, agents etc.) Operator will reimburse TAA in the amount of the civil penalty assessed plus any costs for defending the civil penalty, including reasonable attorneys' fees. TAA will provide Operator notice of the allegation, investigation or proposed or actual civil penalty. Failure of Operator to reimburse TAA immediately upon receipt of such written notice of the assessed civil penalty shall be an event of default.

16. Right of Amendment. Operator agrees that this Agreement may be unilaterally modified by TAA in order to conform to judicial, United States Department of Homeland Security, Federal Trade Commission, Federal Aviation Administration, or other applicable local, state, or federal regulations, legal rulings, or opinions. This section shall not preclude Operator from contesting said rulings or opinions, but Operator and its employees shall abide by the unilateral change. Except as otherwise specifically provided in this Agreement, this Agreement may not be modified except in writing and signed by both parties.

17. Operator Representative. Operator's representative whom TAA may contact to remedy any problem that may arise during the course of this Agreement:

Name: _____
Address: _____
Phone: _____
Email: _____

18. Notice. Notices to TAA are sufficient if hand delivered or sent by certified mail, return receipt requested, postage prepaid, addressed to:

Tucson Airport Authority
Concessions Department
7250 South Tucson Boulevard, Suite 300
Tucson, Arizona 85756
ATTN: Director of Properties and Concessions
CC: Legal Department

Notices to Operator shall be sufficient if hand delivered or sent by regular or certified mail, postage prepaid, to:

Name: _____
Address: _____
Phone: _____
Email: _____

19. Severability at TAA's Option. In the event that any portion of this Agreement, or any action of TAA in support thereof, is declared unconstitutional, unlawful or invalid for any reason by the valid judgment or decree of any court of competent jurisdiction, TAA, in its sole discretion, and without liability to Operator, may either terminate this Agreement in its entirety or treat said unconstitutional, unlawful or invalid portion as severable and continue any remaining valid portions of this Agreement or ordinances in support thereof, in full force and effect.

20. Non-Exclusive Agreement. Operator hereby acknowledges that the rights and privileges authorized herein are non-exclusive. Nothing herein shall be construed to limit TAA's ability to issue permits to other companies providing Services at the Airport.

21. Variance; No Waiver. TAA may grant reasonable variances or adjustments from any term or condition imposed herein. The granting of such a variance shall not operate to waive any of the terms or conditions herein for any purpose except as to the particular provision hereof covered by the variance, and only for so long as the special circumstances warranting the variance exist. The waiver of, or failure to enforce any breach or violation of any term or condition herein contained shall not be deemed to be a waiver or abandonment of such rule or regulation, or a waiver of the right to enforce any subsequent breach or violation of such terms or conditions.

22. Choice of Law & Venue. This Agreement is governed by the laws of the State of Arizona, without regard to any choice of law provisions thereunder. Any action or claim related to this Agreement by any party shall be brought in the courts of the County of Pima, State of Arizona.

This Agreement shall be in full force and effect only when it has been executed by officials of the parties duly authorized to do so.

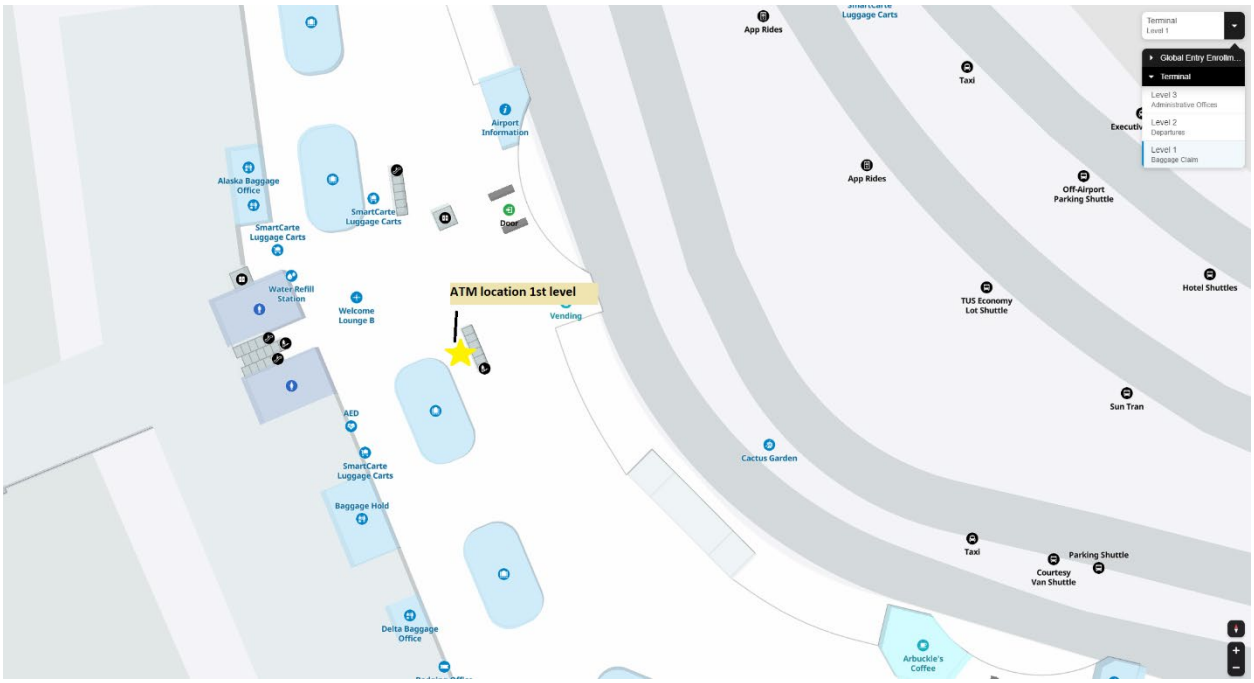
Dated effective as of Effective Date above.

TAA:	**OPERATOR:**
TUCSON AIRPORT AUTHORITY, INC., an Arizona nonprofit corporation	
By: _____	By: _____
Name: John Voorhees	Name: _____
Title: V.P., Chief Revenue Officer	Title: _____
Date: _____	Date: _____

EXHIBIT B - PREMISES

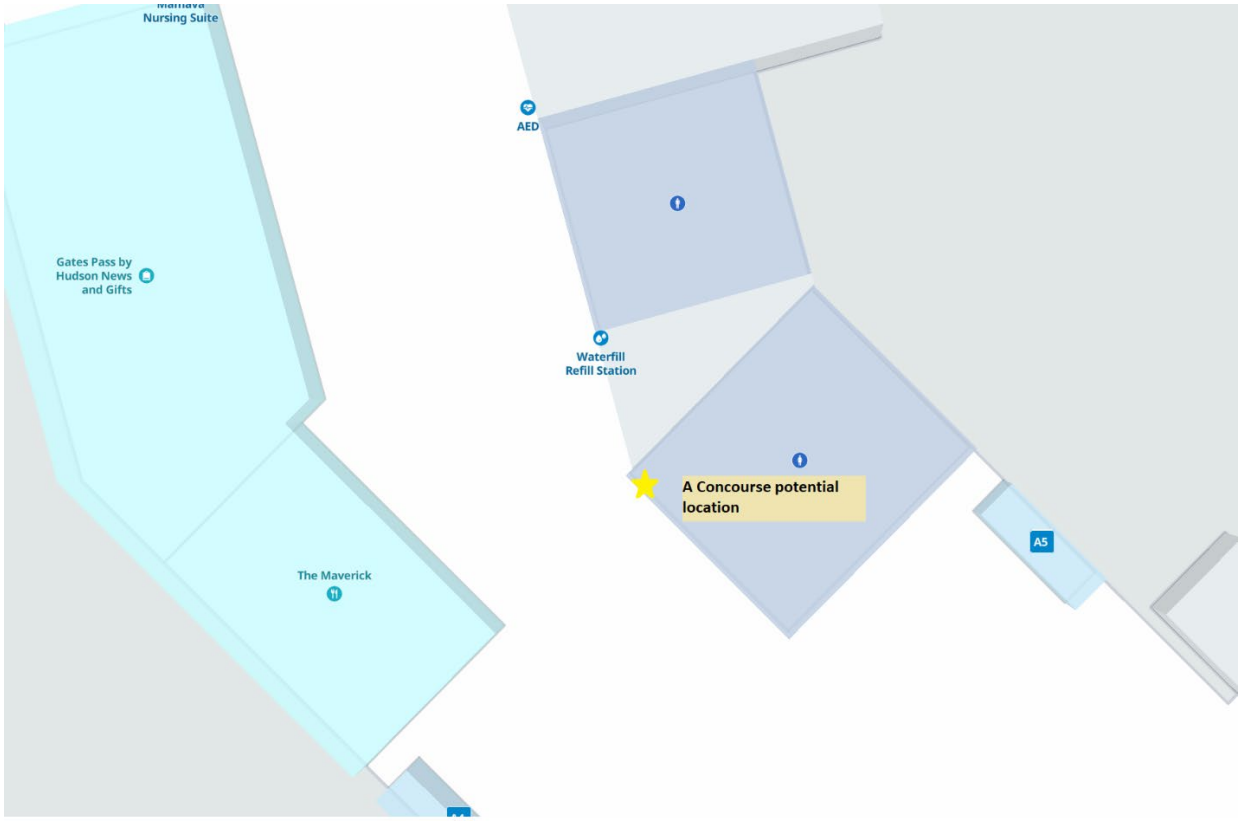
EXHIBIT B - ATM LOCATIONS "PREMISES"

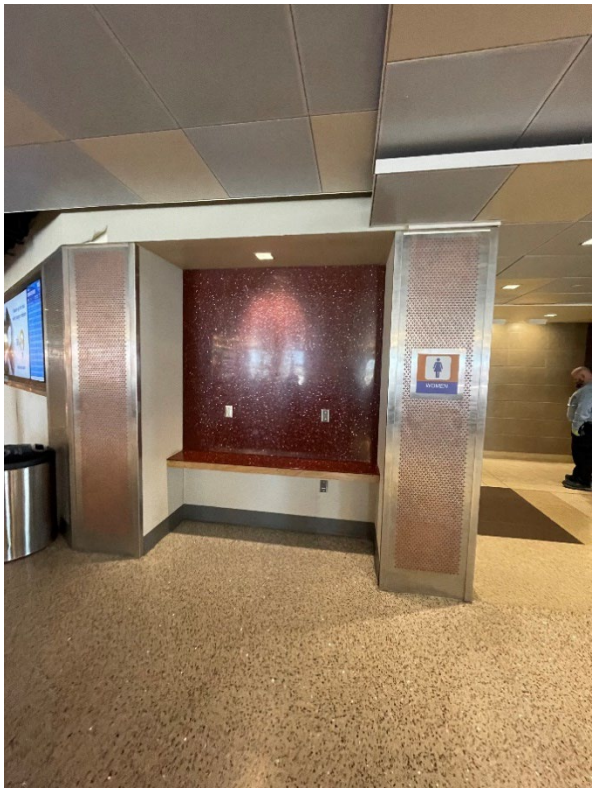
1st Floor Location – Pre-security



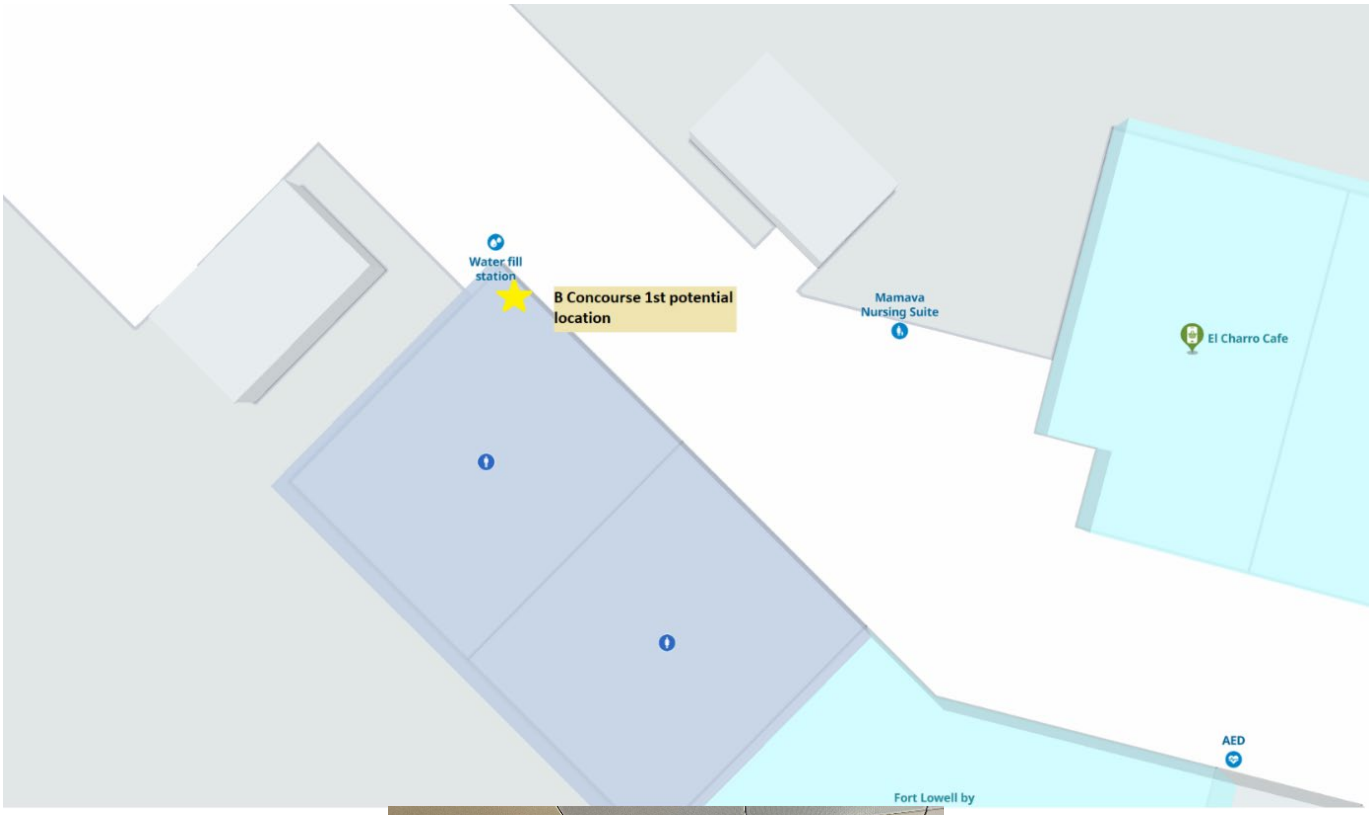
2nd Floor Location - Pre-security

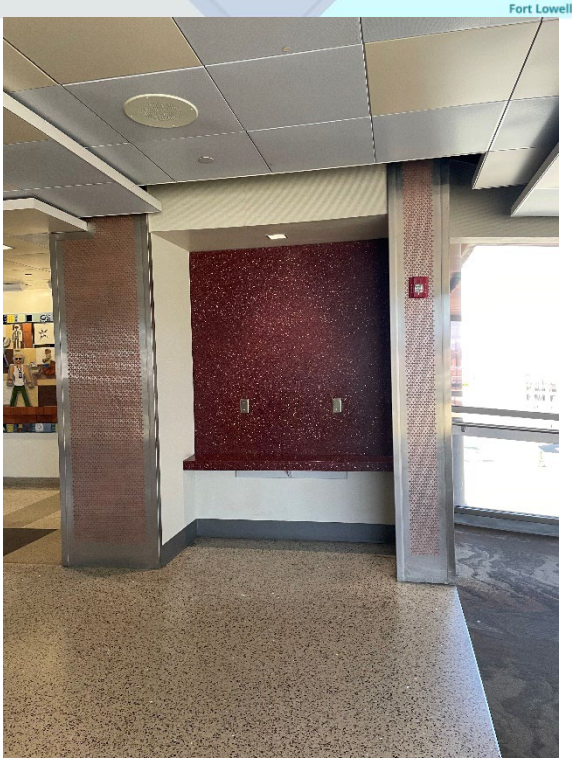
Potential Post-Security ATM Locations
A Concourse - Potential location





Potential Post-Security ATM Locations
B Concourse - Potential Location 1





B Concourse - Potential Location 2

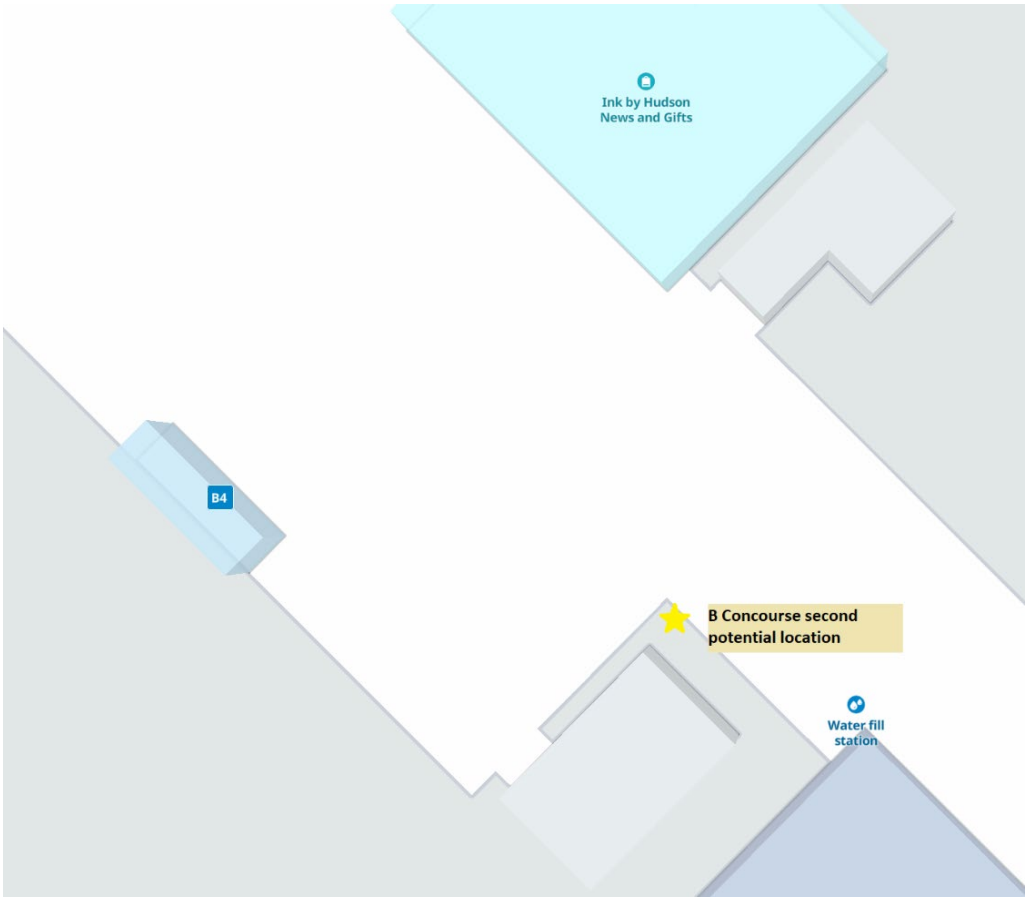


EXHIBIT C - INSURANCE REQUIREMENTS

Operator shall procure and maintain throughout the term of this Agreement insurance against claims for injury to persons or damage to property which may arise from or in connection with the services performed hereunder by Operator, its authorized drivers, agents, representatives, employees, or subcontractors.

The insurance requirements herein are minimum requirements for this Agreement and in no way limit the indemnity covenants contained in this Agreement. TAA in no way warrants that the minimum limits contained herein are sufficient to protect Operator or any Authorized Driver from liabilities that might arise out of the services performed under this Agreement by the Operator, Authorized Drivers, its agents, representatives, employees or subcontractors, and Operator is free to purchase such additional insurance as may be determined necessary.

MINIMUM SCOPE AND LIMITS OF INSURANCE

Operator shall provide coverage at least as broad and with limits of liability not less than those stated below.

1. Commercial General Liability - Occurrence Form

(Form CG 0001, ed. 10/93 or any replacements thereof)

General Aggregate	$1,000,000
Products-Completed Operations Aggregate	$1,000,000
Personal & Advertising Injury	$1,000,000
Each Occurrence	$1,000,000
Uninsured/Underinsured Motorist	$300,000
Fire Damage (any one fire)	$50,000
Medical Expense (any one person)	Optional

Automobile Liability
(Form CA 0001, ed. 12/93 or any replacements thereof)
Combined Single Limit Per Accident for Bodily Injury and Property Damage
$1,000,000

Workers' Compensation and Employer's Liability
Workers 'Compensation: Statutory
Employer's Liability: Each Accident
$1,0000,0000
Disease-Each Employee $1,000,000 Disease-Policy Limit
$1,000,000

SELF-INSURED RETENTIONS OR DEDUCTIBLES
Any self-insured retentions and deductibles must be declared to and approved by TAA.

OTHER INSURANCE REQUIREMENTS

The policies are to contain, or be endorsed to contain, the following provisions:

Commercial General Liability and Automobile Liability Coverages

TAA and the City of Tucson, and each of their officers, officials, agents, employees, and volunteers are additional insureds with respect to liability arising out of: activities performed by or on behalf of Operator, including TAA's general supervision of the Operator; products and completed operations of Operator. Automobile liability coverage to also provide blanket coverage for Operator affiliate vehicles while on airport premises.

Operator's insurance shall contain broad form contractual liability coverage.

TAA, its officers, officials, agents, employees, and volunteers shall be additional insureds to the full limits of liability purchased by Operator even if those limits of liability are in excess of those required by this Agreement or state statute.

Operator's insurance coverage shall be primary insurance with respect to TAA, its officers, officials, agents, employees, and volunteers. Any insurance or self- insurance maintained by TAA, its officers, officials, agents, employees, and volunteers shall be in excess to the coverage of the Operator's insurance and shall not contribute to it.

Operator's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.

Coverage provided by Operator shall not be limited to the liability assumed under the indemnification provisions of this Agreement.

The policies shall contain a waiver of subrogation against TAA, its officers, officials, agents, employees, and volunteers for losses arising from services performed by Operator under this Agreement.

Worker's Compensation and Employer's Liability Coverage

The insurer shall agree to waive all rights of subrogation against TAA, its officers, officials, agents, employees, and volunteers for losses arising from operations work performed by the Operator under this Agreement.

NOTICE OF CANCELLATION

Each policy of insurance required hereunder shall provide for not less than thirty (30) days' notice to TAA before such policy may be canceled or modified in such a way to reduce the coverage provided by the insurance policy or increase any applicable deductible under the policy. Such notice shall be sent by certified mail, return receipt requested.

ACCEPTABILITY OF INSURERS

Insurance is to be placed with insurers duly Agreement or eligible unlicensed companies in the State of Arizona and with a "Best's" rating of not less than A- VII. TAA in no way warrants that the above-required minimum insurer rating is sufficient to protect Operator from potential insurer insolvency.

VERIFICATION OF COVERAGE

Operator shall furnish TAA with Certificates of Insurance (ACORD form) as required by this Agreement. The certificates for each insurance policy are to be signed by a person authorized by that insurer to bind coverage on its behalf.

All certificates are to be received and approved by TAA before services commence. Each insurance policy required by this Agreement must be in effect at or prior to commencement of services under this Agreement and remain in effect for the duration of the Agreement. Failure to maintain the insurance policies as required by this Agreement or to provide evidence of renewal is a material breach of the Agreement.
All certificates required by this Agreement shall be sent directly to:
Tucson Airport Authority
7250 S. Tucson Blvd., Suite 300
Tucson, Arizona 85756

ATTN: Concessions Department

TAA reserves the right to require complete, certified copies of all insurance policies and endorsements required by this Agreement in the event that TAA receives a claim that may trigger the coverage provided by Operator under this Agreement.

APPROVAL

Any modification or variation from the insurance requirements in this Agreement must have prior approval from TAA, whose decision shall be final. Such action will not require a formal contract amendment but may be made by administrative action.

EXHIBIT C

TO
CONCESSIONS AGREEMENT
BETWEEN
TUCSON AIRPORT AUTHORITY
AND

_____

INFORMATION SECURITY REQUIREMENTS

These Information Security Requirements do not replace the vendor's standard policies and procedures but address the minimum information security policies and procedures TAA requires the vendor must have as part of vendor's Service to TAA under this Agreement.

All Information Security Requirements also apply to vendor's subcontractors that have, process, or otherwise have access to TAA Confidential Information and/or TAA Systems.

Any required policies, procedures, or processes mentioned in this Addendum must be documented, reviewed, and approved, determined in writing to be in compliance with this Addendum requirements by TAA IT with designation of Vendor's responsible party conducting management oversight, on a periodic basis, and are hereby incorporated into this Agreement as if fully set forth herein.

DEFINITIONS

TAA	Tucson Airport Authority
Vendor	Any 3rd party company doing business with TAA
TAA Systems	Any Information or Operation Technology owned and operated by TAA or a designated 3rd party vendor at TAA
TAA Confidential Information	Data that TAA determines is not subject to any applicable public records law or protected from disclosure under any other applicable law.
TAA Data	Shall include any electronic information maintained by TAA including, but not limited to, information related to its finances, taxes, employees, customers, tenants, vendors, contractors, and TAA.
Agreement	Negotiated and legally binding arrangement between parties
SOC 2	SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. Type 2 details the operational efficiency of these systems.
ISO 27001	ISO 27001, formally known as ISO/IEC 27001:2022, is an information security standard created by the International Organization for Standardization (ISO), which provides a framework and guidelines for establishing, implementing, and managing an information security management system (ISMS).

FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
FISMA	The Federal Information Security Management Act (FISMA) was enacted in 2002, and requires all federal agencies "to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency."
PCI SSC	Payment Card Industry Data Security Standard
PCI-DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard administered by the Payment Card Industry Security Standards Council that is for organizations that handle branded credit cards from the major card schemes.
PCI-PA-DSS	PCI Payment Application Data Security Standard
HIPAA	Health Insurance Portability and Accountability Act of 1996
PII	Personal Identifiable Information
PHI	Personal Health Information
ITAR/EAR	International Traffic in Arms Regulations / Export Administration Regulations
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
RTO	Recovery Time Objective
RPO	Recovery Point Objective
Product	That which TAA is procuring from the Vendor.
Penetration Test	A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

Data and Data Security Protection Clause

1. Vendor acknowledges that it may have access to certain TAA computer and communications systems and networks for the purposes set forth in this Agreement. If any data is made available or accessible to Vendor, its employees, agents, or contractors, pertaining to TAA's business or financial affairs, or to Licensee's projects, transactions, clients or customers, Vendor will not store, copy, analyze, monitor, or otherwise use that data except for the purposes set forth in the Agreement for the benefit of TAA.

2. Vendor will comply fully with all applicable laws, regulations, and government orders relating to PII and data privacy with respect to any such data that Vendor receives or has access to under the Agreement or in connection with the performance of any services for Licensee. Vendor will otherwise protect PII and will not use, disclose, or transfer across borders such PII except as necessary to perform under the Agreement or as authorized by the data subject or in accordance with applicable law.

3. To the extent that Vendor receives PII related to the performance of the Agreement, Vendor will protect the privacy and legal rights of TAA's personnel, clients, customers, tenants, and contractors.

4. All right, title, and interest in TAA's Data will remain the property of TAA. Vendor has no intellectual property rights or other claim to TAA's Data that is hosted, stored, or transferred to and from the Products or the cloud services platform provided by Vendor, or to TAA's Confidential Information. Vendor will cooperate with TAA to protect TAA's intellectual property rights and TAA's Data. Vendor will promptly notify TAA if Vendor becomes aware of any potential infringement of those rights in accordance with the provisions of this Agreement.

5. For purposes of this Agreement and the Exhibits attached hereto, all TAA Data stored or at rest within the vendor's data centers or in cloud hosted data centers, in transport, will be encrypted in transport and rest (when regulatorily and/or contractually required) and will not be transferred to any other hosting entity or location without the prior written consent of TAA.

Data Safeguards Clause

1. Vendor has represented to TAA that the Vendor will not be permitted to access TAA Data stored or contained in the Products or Vendor's platform, and Vendor will have no ability to manipulate, modify or control such TAA Data. If any support services or Professional Services provided by Vendor may involve Vendor or its personnel having or requiring access to TAA's servers, applications, and/or Data, Vendor shall comply with the provisions of this Section and Exhibit A attached hereto, and, at TAA's request, Vendor shall enter into an appropriate separate agreement with TAA to govern such access and protect any TAA Data that may be subject to such access. To the extent TAA grants Vendor access to TAA Data, or Vendor has access to or stores or holds any TAA Data, Vendor agrees to:

    (i) access and use the TAA Data solely for the purpose of providing TAA with access to the Products, Software and Vendor's platform, and to provide Services to TAA in accordance with the terms and conditions of this Agreement and any applicable Statement(s) of Work;

    (ii) maintain physical, technical, and administrative safeguards (including but not limited to those set forth in this Section, Exhibit A (Data Security) attached to this Agreement, and in any event no less than industry standards in the cloud computing/online services industry) to protect the TAA Data against unauthorized access, use, or disclosure while it is accessible to or held by Vendor ("Data Safeguards"); and

    (iii) not disclose the TAA Data to any third party, except: (i) to its employees, consultants or contractors who need to have access to such information and solely for purposes of providing Services to TAA, provided that such recipients are bound by confidentiality provisions no less restrictive than those set out in this Agreement; and (ii) to the extent required by a judicial order or other legal obligation, provided that, to the fullest extent permitted by law, Vendor will promptly notify TAA of such a required disclosure to allow intervention by TAA (and will cooperate with TAA) to contest or minimize the scope of the disclosure.

Attestations and Certifications

1. Vendor will, on at least an annual basis, hire a third-party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) SOC2 audit, or equivalent audit (ISO 27001, FedRAMP, FISMA), on internal and external Vendor procedures and systems that access or contain TAA Data. Vendor shall adhere to SOC 2 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by TAA), applicable to TAA. Vendor's security procedures will materially conform to the description thereof set forth in this Agreement and in attached Exhibit A (Data Security), and as further described in Vendor's most recently completed security audit report (or any successor report of a similar nature that is generally accepted in the industry and utilized by Vendor).
   The Vendor will also provide access to the certifications required via written request from TAA.
   TAA has the right to perform a due diligence assessment to validate the cyber hygiene of the supplier/Vendor.

2. Additionally, if any regulated data is being processed, the vendor will also provide the appropriate certification (PCI SSC/ PCI-DSS / PCI-PA-DSS for credit card data and HIPAA for any healthcare information) in addition to the SOC2 type to or equivalent audit certification.
   Each certification will also provide a date of expiration, where at that date/time, the most recent and active certification will be provided to the TAA.

3. Upon TAA's request, Vendor will provide TAA with a copy of the security certifications and results of the attestation audit.

Data Breach Notification

1. If the vendor suspects or becomes aware of any unauthorized access to any TAA Data or Personal Data by any unauthorized person or third party, or becomes aware of any other security breach relating to Personal Data held or stored by the vendor under this Agreement or in connection with the performance of the Services or other services performed under this Agreement or any Statement(s) of Work ("Data Breach"), the vendor shall notify the TAA in writing within 24 hours and shall fully cooperate with TAA at the vendor's expense to prevent or stop such Data Breach and any consequential impacts to TAA and its Board, employees and Members following the breach.

2. In the event of such Data Breach, vendor shall fully and immediately comply with applicable laws, and shall take the appropriate steps to remedy such Data Breach.

3. The vendor will, to the fullest extent permitted by law, defend, indemnify and hold TAA, its Affiliates, and their respective officers, directors, employees and agents, harmless for, from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorney fees, arising out of or relating to any third party claim arising from breach by the vendor of its obligations contained in this Section, except to the extent resulting from the negligent or willful acts or omissions of TAA.

4. All Personal Data to which the vendor has access under this Agreement, as between the vendor and TAA, will remain the property of TAA and will follow the provisions of TAA data with additional security controls to protect the data accordingly to HIPAA, PCI, and other regulatory requirements.

5. TAA hereby consents to the use, processing and/or disclosure of Personal Data only for the purposes described herein and to the extent such use or processing is necessary for the vendor to carry out its duties and responsibilities under this Agreement, any applicable Statement(s) of Work, or as required by law.

6. The vendor will not transfer any data deemed sensitive (PII, PHI, ITAR/EAR, Confidential, etc.) by TAA to third parties other than through its underlying network provider to perform its obligations under this Agreement. All TAA data delivered to the vendor shall be stored in the United States or other jurisdictions approved by TAA in writing and shall not be transferred to any other countries or jurisdictions without the prior written consent of TAA.

Business Continuity/Disaster Recovery; Flip-Over Rights

1. Vendor represents and warrants that its enterprise Business Continuity Program (BCP) is ISO 22301 certified. The vendor shall also comply with the business continuity requirements set forth with the client.

2. TAA may exercise Flip-Over Rights (as defined below) at any time during the period that the vendor fails to restore Services in accordance with the applicable and approved BCP and included RTO(s) (Recovery Time Objective) and, upon written request cannot provide adequate assurances that restoration of services will occur reasonably soon (as reasonably determined by TAA), and, in doing so, may take other action as is reasonably necessary to provide similar services during the period the Services are disrupted. The vendor shall cooperate with TAA and its agents, as applicable, in the exercise of such Flip-Over Rights and provide reasonable assistance at no charge to TAA to promptly restore such disrupted Services.

3. The vendor shall not be entitled to receive any payments to the extent they relate to Services performed by TAA and all costs associated with the exercise of such Flip-Over Rights shall be borne by Vendor. Such Flip-Over Rights shall continue until Vendor demonstrates to TAA's reasonable satisfaction that Vendor is able to resume performance of the Services with appropriate mitigation in place designed to prevent further BCP failures for the Services. Such exercise of Flip-Over Rights shall not constitute a waiver by TAA of any termination rights or rights to pursue a claim for damages arising out of the failure that led to the Flip-Over Rights being exercised.

4. Flip-Over Rights shall mean that TAA may use its own proprietary tools and/or another website or websites to provide information to Vendor as TAA may determine is reasonably under the circumstances.

EXHIBIT A - Data Security

Notwithstanding anything to the contrary contained in the Master Services Agreement to which this Exhibit is attached ("Agreement"), and all other Exhibits thereto, and in addition to and not in lieu of other provisions in the Agreement and the Exhibits thereto, the vendor agrees as follows:

1. General Security Procedures

1.1 Without limiting Vendor's obligation of confidentiality as further described in the Agreement and herein, Vendor will be responsible for establishing and maintaining an information security program that is designed to:

(i) ensure the security and confidentiality of TAA Data;

(ii) protect against any anticipated threats or hazards to the security or integrity of the TAA Data;

(iii) protect against unauthorized access to or use of the TAA Data;

(iv) ensure the proper disposal of TAA Data, as further defined herein; and

(v) ensure that all subcontractors of Vendor, if any, comply with all of the foregoing. Vendor will designate an individual to be responsible for the information security program. Such individual will respond to TAA inquiries regarding computer security and to be responsible for notifying TAA-designated contact(s) if a breach or an incident occurs, as further described herein. The information security program will be audited annually as detailed in Vendor's SOC2 or equivalent audit reports, which will be made available to TAA upon request.

(vi) ensure that the Vendor is maintaining a vulnerability management program which prioritizes by risk, regularly reviews, and analyzes threat intelligence to identify vulnerable software with remediations for Critical and High vulnerabilities remediated within 30 days of software, firmware, patch release.

1.2 Vendor must conduct formal security awareness training, with a testing component, for all personnel and contractors as soon as reasonably practicable after the time of hiring or prior to being appointed to work on TAA Data and annually recertified thereafter. Documentation of Security Awareness Training must be retained by Vendor, confirming that this training and subsequent annual recertification process have been completed, and available for review by TAA.

1.3 TAA will have the right to review Vendor's information security program prior to the commencement of TAA's entry of data into the Product(s) or delivery to TAA of any Professional Services and from time to time during the Term of this Agreement. During the Term of the Agreement, from time to time with proper notice and Vendor approval, which will not be unreasonably withheld, TAA, at its own expense, will be entitled to perform, or to have performed, an on-site or virtual audit of Vendor's information security program and facilities. In lieu of an on-site audit, upon request by TAA, Vendor will use reasonable efforts

to complete, within forty-five (45 days) of receipt, an Information Security Assessment questionnaire provided by TAA regarding Vendor's information security program.

1.4 In the event of any actual or apparent theft, unauthorized use or disclosure of any TAA Data, Vendor will immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and within three (3) business days 72 hours following discovery of any such event, provide TAA notice thereof, and such further information and assistance as may be reasonably requested.

1.5 TAA Data, including but not limited to sales data, hosted, stored, or held by Vendor in the Product(s) or in the platform operated by Vendor, or on any device owned or in the custody of Vendor, its employees, agents, or contractors, will be encrypted. Vendor will not transmit any unencrypted TAA Data over the internet or a wireless network and will not store any TAA Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by TAA in writing.

1.6 The parties acknowledge and agree that any disclosure of TAA Data will in no way be construed to be an assignment, transfer, or conveyance of title to or ownership rights in such TAA Data.

2. Network and Communications Security

2.1 All Vendor connectivity to TAA computing systems and all attempts at same will be only through TAA's security gateways/firewalls/VPN and only through TAA approved security procedures.

2.2 Vendor will not access, nor permit unauthorized persons or entities to access, TAA computing systems and/or networks without TAA's express written authorization, and any such actual or attempted access will be consistent with any such authorization.

2.3 Vendor will take appropriate measures to ensure that Vendor's systems connecting to TAA's systems, and anything provided to Vendor through such systems do not contain any Disabling Device. For purposes of this Agreement, "Disabling Device" means any programs, mechanisms, programming devices, malware or other computer code (i) designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", "spyware", "viruses" or "worms"); (ii) that would disable or impair the operation thereof or of any software, computer system or network in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", "time locks", or "drop dead" devices); (iii) is designed to or could reasonably be used to permit a party or any third party to access any computer system or network (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (iv) is designed to or could reasonably be used to permit a party or any third party to track, monitor or otherwise report the operation and use of any software program or any computer system or network by the other party or any of its customers.

3. Customer Data Handling Procedures

3.1 Erasure of Information and Destruction of Electronic Storage Media. If TAA Data is required to be permanently deleted from any storage media owned or operated by Vendor, all electronic storage media containing Customer Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization.

3.2 Vendor must maintain documented evidence of data erasure and destruction. This evidence must be available for review at the request of TAA for the length of the contract period.

4. Physical Security

4.1 All backup and archival media containing TAA Data must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by Vendor and all backup and archival media containing TAA Data must be encrypted. Data restoration times will be defined within the service level agreement and will be mutually agreed upon by both the TAA and the vendor. Data that is exported out of designated data stores will be limited except upon expiration/termination of the Agreement. If due to cloud configurations, the data may leave the United States, written approval is required by TAA to ensure that the data can be exported outside US territory. TAA reserves the right to inspect physical site and security controls annually as a part of the product and/or service being received by TAA. All TAA Data held by Vendor will be accessible/recoverable by TAA prior to expiration/termination of the Agreement.

5. Penetration Testing

5.1 Vendor will provide TAA with an annual, third-party Penetration Test report. During the term of this Agreement, Vendor will engage, at its own expense and at least one time per year, a third-party vendor reasonably acceptable to TAA to perform penetration and vulnerability testing ("**Penetration Tests**") with respect to Vendor's systems.

5.2 The objective of such Penetration Tests is to identify design and/or functionality issues in infrastructure of Vendor's systems that could expose TAA Data and its computer and network equipment and systems to risks from malicious activities. Penetration Tests will probe for weaknesses in network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to Vendor's systems that could be exploited by a malicious party.

5.3 Penetration Tests will identify, at a minimum, the following security vulnerabilities: invalidated or un-sanitized input; broken access control; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; denial of service; insecure configuration management; proper use of SSL/TLS; proper use of encryption; remote code execution; social engineering, network and anti-virus reliability and testing and more to effectively understand the capabilities in place and any potential vulnerabilities that may pose a risk to the delivery of the product and/or service.

5.4 Within a reasonable period after the annual Penetration Test has been performed, TAA will receive from Vendor a report of any high level and medium level security issues that were revealed during such Penetration Test and subsequent certification in writing to TAA that such high level and medium level security issues have been fully remediated.

5.5 To the extent that high level and/or medium level security issues were revealed during a particular Penetration Test, Vendor will subsequently engage, at its own expense, an additional Penetration Test within a reasonable period thereafter to ensure continued resolution of identified security issues and will notify TAA with the results thereof.

6. **Background Checks**

6.1 Vendor will not assign any employee to perform services for TAA who has not authorized a background investigation, or whose background investigation has revealed the conviction of a felony or misdemeanor within the previous ten (10) years, measured back from the time such Vendor employee commences services pursuant to the Agreement, to the extent such felony or misdemeanor relates to the suitability of the individual's employment, except to the extent prohibited by applicable law.

6.2 If Vendor contracts, for any services, with a third party that needs to be allowed or requires access to TAA Data, the third party will undergo the same Vendor background checks as performed on Vendor personnel and contractors under this section.

7. **Lack of Certifications or Security Program Attestation**

7.1 TAA shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that Vendor fails to produce an acceptable certification or attestation in which the original claims of the service were covered.

7.2 TAA reserves the right to contract with any vendor of its choosing in order to preserve, support and protect the operations of TAA related to the Services provided under this Agreement.