



Procurement and Contracting Services

Request for Proposals for Point of Sale and eCommerce Solution

**Please mark all proposal submission
Files with the following information**

Sealed RFP # L302604
Due on April 30th, 2026 **no later than 1:00 PM, MST**

TABLE OF CONTENTS
For
REQUEST FOR PROPOSALS NO. L302604

SECTION #	TITLE
1.0	<u>Statement of Work</u>
2.0	<u>Definitions</u>
3.0	<u>General Information and Instructions to Proposers</u>
4.0	<u>Agreement Terms and Conditions</u>
5.0	<u>Scope of Work, Specifications, Technical Requirements</u>
6.0	<u>Certifications and Forms</u> (Vendor to complete and return with proposal)



PROCUREMENT AND CONTRACTING SERVICES REQUEST FOR PROPOSALS, RFP #L302604

1.0 STATEMENT OF WORK

1.1 Summary

The Arizona Board of Regents (ABOR), on behalf of the University of Arizona, is soliciting proposals from interested vendors to furnish the University with a native Point of Sale (POS) and native eCommerce solution.

The University of Arizona Campus Store (“Campus Store”) operates a mission-critical retail environment serving 45,000+ students, faculty, and staff across multiple locations. The current ecosystem includes NetSuite Point of Sale (NSPOS) and Suite Commerce eCommerce, which are being sunset by Oracle in 2027. Oracle NetSuite ERP will continue to be the single source of truth for inventory, pricing, customer records, and financial data for the foreseeable future.

The Arizona Board of Regents (ABOR), on behalf of the University of Arizona, is soliciting proposals from interested vendors to furnish the University with a single platform that provides a native Point of Sale (POS) and native eCommerce functionality, supported by supplier-hosted website infrastructure, within the same solution, providing both in-store and online transactions. The solution must provide integrated product catalog, inventory management, and order management across POS and eCommerce channels. Since the university will retain its current ERP, the proposed solution must support API integration for financial and operational data exchange.

- 1.2 Coverage and Participation.** The intended coverage of this RFP and any Agreement resulting from this solicitation shall be for the use of all Departments at the University of Arizona. The other State Universities: Arizona State University (ASU) and Northern Arizona University (NAU), along with Pima Community College (PCC) and any other educational institution or Governmental entity, may access an Agreement resulting from this solicitation issued and administered by the University of Arizona.

2.0 DEFINITIONS

- 2.1 Agreement / Contract.** All types of agreements entered into by the Arizona Board of Regents, regardless of what they may be called, for the procurement of materials, services or construction, or the disposal of materials. Meaning is interchangeable.
- 2.2 Customer.** Unless otherwise implied by the context of the specific provision within this RFP, "Customer" means a customer of the vendor, other than the University.
- 2.3 Contractor.** Same as Successful Vendor.
- 2.4 May, Should.** Indicates something that is not mandatory but permissible, recommended or desirable.
- 2.5 MST. Mountain Standard Time.** Arizona does not observe Daylight Savings Time.
- 2.6 Must, Shall, Will.** Indicates a mandatory requirement. Failure to meet these mandatory requirements may result in the rejection of your proposal as non-responsive.

- 2.7 Proposal.** The entirety of the vendor's responses to each point of this RFP, including any and all supplemental offers or information not explicitly requested within this RFP.
- 2.8 Proprietary Information.** Information held by the owner that if released to the public or anyone outside the owner's organization, would be detrimental to its interests. It is an issue of fact rather than opinion. Pricing and/or revenues cannot be considered proprietary or confidential.
- 2.9 Provider.** Same as Vendor.
- 2.10 Request for Proposals (RFP).** A competitive process under which discussions and negotiations are allowed, it is not to be confused with a Request for Bid (RFB), in which goods or services are precisely specified and price is substantially the only competitive factor. This RFP provides the University the flexibility to negotiate to arrive at a mutually agreeable relationship. Price will be considered, but will not be the only factor of evaluation.
- 2.11 Respondent.** Same as Vendor
- 2.12 Response.** Same as Proposal.
- 2.13 Responsible Vendor.** A person who has the capability, including necessary experience, to perform the contract requirements; who has the integrity and reliability which will ensure good faith performance and appropriate quality of the materials, services, construction or construction services, to be provided; and who is in compliance with any and all licensing requirements of the State of Arizona.
- 2.14 Responsive Vendor.** A person who submits a proposal which conforms in all material respects to the Request for Proposals.
- 2.15 Successful Vendor.** Any vendor selected by the University to receive a notice of award as a result of this RFP and to enter into a contract to provide the University with the products or services sought by this RFP
- 2.16 Supplemental Agreement.** Any supplemental terms and conditions agreed to by the parties in writing, which take precedence over all other documents governing the transaction.
- 2.17 Supplier.** Same as Vendor.
- 2.18 University. Arizona Board of Regents (ABOR),** a body corporate, for and on behalf of the University of Arizona.
- 2.19 Vendor.** For purposes of this RFP, "Vendor" means any entity responding to this RFP with the intention of winning the resulting award of contract, performing the work, and/or delivering the goods specified herein.
- 2.20 Vendor's Proposal.** Same as Proposal.
- 2.21 Vendor's Response.** Same as Proposal.

3.0 GENERAL INFORMATION AND INSTRUCTIONS TO PROPOSERS

- 3.1 Original RFP Document.** The Office of Procurement and Contracting Services shall retain the RFP, and all related terms and conditions, exhibits and other attachments, in original form in an archival copy. Any modification of these, in the vendor's submission, is grounds for immediate disqualification.
- 3.2 About the University.** For information about the University of Arizona, please visit the University's Internet web page at: www.arizona.edu. For specific demographic information, visit <https://uair.arizona.edu/content/overview>.

University Purpose and Core Values. The University of Arizona's purpose is working together to expand human potential, explore new horizons and enrich life for all. To fulfill this purpose, the University has adopted Core Values that apply to all faculty, staff, and students, as well as to those doing business with the University. The Core Values are

central to the culture of the University, and Vendors are encouraged to review and uphold the following:

- Integrity – Be honest respectful and just
- Compassion – Choose to Care
- Exploration – Be insatiably curious
- Adaptation – Stay open-minded and eager for what's next
- Inclusion – Harness the power of diversity
- Determination – Bear Down

For additional information regarding the University's Purpose and Core Values, please visit <https://www.arizona.edu/purpose-values>.

3.3 Schedule of Events. The following is the tentative schedule that will apply to this RFP, but may change in accordance with the University's needs.

03-31-26	Issuance of RFP
04-10-26	Supplier Questions Due by 1:00pm MST
04-30-26	Proposals Due, No Later than 1pm MST
TBD	Presentations/ Software demonstrations (if selected)
TBD	Sandbox Evaluation (if selected and if applicable)

3.4 Pre-Proposal Conference. Intentionally Omitted

3.5 Pre-Proposal Site Visit. Intentionally Omitted

3.6 Accommodations for People with Disabilities. If the vendor or any of the vendor's employees participating in this RFP need, or have questions about the University's accommodations for people with disabilities, please make arrangements with:

Zane Forier
Phone: 520-626-2405
Email: zforier@arizona.edu.

Such requests should be made as early as possible to allow time to arrange the accommodation(s).

3.7 PROPOSAL PREPARATION INSTRUCTIONS

3.7.1 Vendor's Understanding of the RFP. In responding to this RFP, the vendor accepts the responsibility fully to understand the RFP in its entirety, and in detail, including making any inquiries to the University as necessary to gain such understanding. The University reserves the right to disqualify any vendor who demonstrates less than such understanding. Further, the University reserves the right to determine, at its sole discretion, whether the vendor has demonstrated such understanding. Related to this, the University's right extends to cancellation of award if award has been made. Such disqualification and/or cancellation shall be at no fault, cost, or liability whatsoever to the University.

3.7.2 University Provides Information in Good Faith without Liability. All information provided by the University in this RFP is offered in good faith. Individual items are subject to change at any time. The University makes no certification that any item is

without error. The University is not responsible or liable for any use of the information, or for any claims attempted to be asserted therefrom.

3.7.3 Verbal versus Written Communication. Verbal communication shall not be effective unless formally confirmed in writing by the specified University procurement official in charge of managing this RFP's process. In no case shall verbal communication override written communication.

3.7.4 Questions, Communications and Inquiries between the University and Vendors. All Vendor inquiries, questions and requests for clarification related to this RFP are to be directed, in writing via email, ONLY to the Buyer listed below. Once this RFP has been issued, Vendors are not to contact any University Department, other than Procurement and Contracting Services, concerning this RFP, or risk disqualification (see Section 3.7.1 above):

Attn: Zane Forier
Telephone No. 520-626-2405
Email Address: zfforier@arizona.edu

Applicable terms and conditions herein shall govern communications and inquiries between the University and vendors, as they relate to this RFP.

Informal communications shall include but are not limited to requests from/to vendors or vendors' representatives of any kind or capacity, to/from any University employee or representative of any kind or capacity, **with the exception of the Purchasing Department**, for information, comments, speculation, etc. Inquiries for clarifications and information that will not require addenda may be submitted verbally to the Buyer named above, at any time.

Formal communications shall include but are not limited to the following.

- Questions concerning this RFP must be submitted in writing, and be received **no later than April 10th 2026**.
- Errors and omissions in this RFP and enhancements. Vendors shall bring to the University's attention any discrepancies, errors, or omissions that may exist within this RFP. Vendors shall recommend to the University any enhancements in respect to this RFP, which might be in the University's best interests. These must be submitted in writing, and be received **no later than April 10th 2026**.
- Inquiries about technical interpretations must be submitted in writing, and be received **no later than April 10th 2026**.
- Inquiries for clarifications / information that will **not** require addenda may be submitted verbally to the Buyer named above at any time during this process.
- Verbal and/or written presentations and pre-award negotiations under this RFP.
- Addenda to this RFP.

Informal communications shall cease on the date of distribution of this RFP and formal communications shall commence. On the date that the University notifies responding vendors of this RFP's results and executes the resulting contract with the successful Vendor, informal communications may resume and formal communications may cease.

3.7.5 Addenda and the University's Response to Communications from Vendor. The University will make a good-faith effort to provide a written response to each question or request for clarification that requires addenda within five (5) University business days.

All addenda will be posted to our web site: <https://vendors.arizona.edu/rfpb-opportunities>

Vendors who want the addenda supplied to them in another form must notify **Zane Forier**. Otherwise, it is the vendor's responsibility to check the web site for any additional information and addenda concerning this RFP.

The University will not respond to any questions / requests for clarification that require addenda, if received by the University after **April 10th 2026**.

3.7.6 Pricing and/or Revenue Proposal. Vendors shall indicate pricing and/or revenue offers in the appropriate spaces and/or areas provided in this RFP. The University may presume and hold as the vendor's final offer all pricing and/or revenue offerings, whether stated as amounts or percentages, and/or whether or not offered on an all-or-none basis, if not specified by the vendor. The University may accept or reject in part or entirely the vendor's pricing and/or revenue offerings when such offerings are not on an all-or-none basis. Vendor's pricing and/or revenue proposals may not be modified after the RFP Due date and time unless University at its sole discretion decides that future negotiations will only enhance the Vendor's offer to University. Should University decide that such negotiations would not be in University's best interests, pricing and revenue offer by Vendor at Due date and time may be considered by University as the Vendor's best and final offer. Unless otherwise specifically proposed by the vendor, the University reserves the right to hold such pricing and/or revenue proposal as effective for the entire intended contract term. The University may prescribe the manner and method by which pricing and/or revenue offerings shall be communicated in the vendor's proposal. The University may reject any proposal in which the pricing and/or revenue offering does not conform to such prescribed manner and method. Vendors shall indicate pricing and/or revenue offers in the appropriate spaces and/or areas provided in this RFP. Vendors shall ensure that any departure from this condition results in an offer that is clearly cross-referenced to the applicable sections within this RFP. For any material departure from this condition, vendors shall provide clear and unambiguous explanations how the departure relates in detail to the applicable sections within this RFP. If the vendor responds with an "All-or-None" proposal, it shall be clearly and unambiguously marked as such.

3.7.7 Revisions to the RFP. The University may revise any part of this RFP for any reason by issuing addenda. The University will communicate additional information and addenda to this RFP by posting them on our web site: <https://vendors.arizona.edu/rfpb-opportunities>

Vendors are responsible for the information contained in such addenda, whether or not they acknowledge receipt. The University is under no obligation to communicate such addenda to vendors who notify the University that they will not be responding to this RFP. The University may determine whether an addendum will be considered as part of this RFP and/or as part of any resultant contract. The University shall reject vendors' responses to addenda if such responses are received after the RFP Due date and time.

3.7.8 Attention to Terms and Conditions. Vendors are cautioned to thoroughly understand and comply with all matters covered under the Terms and Conditions section of this RFP. The successful Vendor is expected to enter into a form of agreement approved by the Arizona Board of Regents. The University agreement terms and conditions included in this RFP are intended to be incorporated into this agreement.

Proposals that are contingent upon any changes to these terms and conditions may be deemed to be non-responsive and may be rejected.

3.7.9 Required Signatures. The University may reject any vendor's response if it is not signed as indicated and/or required by the areas, spaces, or forms provided within this RFP.

3.7.10 Proposal Organization. Vendors shall present proposals in a format that can be readily incorporated into a contract. Vendors may present narrative proposals provided that such proposals follow the same outline and numbering scheme of this RFP, including full descriptive cross-references to all requirements listed in [Section 5.0](#). Vendors should ensure that their proposals include page numbers and are organized in a manner that will facilitate the University's evaluation of them. **The University reserves the right to reject without prior notice and without liability of any kind or amount any proposal that it deems overly complex, disorganized, or difficult to evaluate.** The University reserves the right to make such a decision without any input or communication from any other party. Vendors shall ensure that, at a minimum, their proposals contain the components set forth in the following list.

- Original required sections from this RFP
- Any additional responses in corresponding sequence order
- Any additional supporting data

3.7.11 Collusion Prohibited. In connection with this RFP, vendor collusion with other vendors or employees thereof, or with any employee of the University, is prohibited and may result in vendor disqualification and/or cancellation of award. Any attempt by the vendor, whether successful or not, to subvert or skirt the principles of open and fair competition may result in vendor disqualification and/or cancellation of award. Such disqualification and/or cancellation shall be at no fault or liability whatsoever to the University.

3.7.12 Improper Business Relationships / Conflict of Interest Prohibited. In connection with this RFP, each vendor shall ensure that no improper, unethical, or illegal relationships or conflict of interest exists between or among the vendor, the University, and any other party to this RFP. The University reserves the right to determine the materiality of such relationships, when discovered or disclosed, whether intended or not; and to decide whether or not vendor disqualification and/or cancellation of award shall result. Such disqualification and/or cancellation shall be at no fault or liability whatsoever to the University.

3.7.13 Corrections, Changes, and Providing Information on Forms within the RFP. Vendors shall ensure that an authorized individual initials each correction using pen and ink. Vendors shall use pen and ink or typewriter in providing information directly on pages, or copies thereof, contained within this RFP.

3.7.14 Proposal Bond. Not Applicable

3.7.15 Performance and / or Payment Bonds. Not Applicable.

3.7.16 Anti-Kickback. In compliance with FAR 52.203-7, the University has in place and follows procedures designed to prevent and detect violations of the Anti-Kickback Act of 1986 in its operations and direct business relationships.

3.8 PROPOSAL SUBMISSION AND SUBSEQUENT ACTION

Proposals must be received by the date / time and uploaded to the University's secure box no later than April 30th 2026 1:00 PM MST.

Vendors, please be advised that it is *your sole responsibility* to ensure that your proposal is received as described in the paragraph above. The University shall not be responsible for any delays that may occur.

Proposals must be uploaded to Box Secure Upload no later than April 30th 2026 1:00 PM MST. at this link: <https://arizona.app.box.com/f/7a51c2adfb6c4e5b8df1bf22ff8769be>

Please title your response in the upload folder as:

RFP L302604_VendorName_Response

****No more than four (4) documents should be uploaded. The uploads should only include the following:**

1. Signed certificates per section 6.0, combined as one file.
2. Narrative proposal per section 5.
3. Completed Attachment A spreadsheet.
4. One combined file for the following items requested in Attachment A:
 - a. Full list of roles and their permissions (Section 1, question 2. Excel row 16)
 - b. Service Level Agreement (Section 2, question 8. Excel row 44)
 - c. Architecture diagram (Section 4, question 11. Excel row 100)
 - d. VPAT (Section 10, question 2. Excel row 152)

****You may include a redacted copy of each file if necessary****

The University shall, at the specified Due date and time, accept all proposals that are otherwise in order. The University will allow interested parties to be present via zoom for purposes of identifying which vendors have responded, if requested. The University will make no immediate decision at such time, and **there will be no disclosure of any information contained in any proposal until after formal notice of award and execution of any contract resulting from this RFP.** When multiple solicitations have been scheduled to open at the same date and time, the University will open solicitations that have interested individuals present in sequential order by solicitation number. **The University will hold unopened any proposals received after the Due date and time, and will not consider such proposals.** The University reserves the right to retain or dispose of such proposals at its discretion; however, the University may return such proposals to their related vendors, but only at such vendor's request and at no cost or expense whatsoever to the University.

If the University determines that due to an insufficient number of proposals received, it would be in the University's best interest, the University may extend the Due date in order to determine why other vendors did not respond and to encourage other vendors to respond.

3.8.1 Proposal Costs. The University is not liable in any manner or to any extent for any cost or expense incurred by any vendor in the preparation, submission, presentation, or any other action connected with proposing or otherwise responding to this RFP. Such exemption from liability applies whether such costs are incurred directly by the vendor or

indirectly through the vendor's agents, employees, assigns or others, whether related or not to the vendor.

3.8.2 Withdrawal of RFP. Vendors may withdraw their proposals any time prior to the RFP Due date and time. Vendors may request to withdraw their proposals after the RFP Due date and any time prior to selection and notice of award. The University shall have sole authority to grant or deny such a request. In the event the University grants such a request, it may withhold issuing future RFP's to such vendors.

3.8.3 University's Right to Use Vendor's Ideas / Proprietary Information. If the vendor needs to submit proprietary information with the proposal, the vendor **shall ensure that it is enclosed in a separate redacted file from the proposal and that it is clearly designated and conspicuously labeled as such. The vendor may submit a full PDF for the committee and a redacted file for proprietary and confidential information within the guidelines below.**

The University shall have the right to use any ideas that are contained in any proposal received in response to this RFP, along with any adaptation of such ideas. Selection or rejection of the proposal shall not affect the University's right of use. Provided, however, that the University will, in good faith, honor any vendor information that is **redacted and saved as a separate file from the proposal and clearly designated and conspicuously labeled as proprietary, and the University concurs that the information is proprietary. The file must also contain the reason(s) why the enclosed material is to be considered proprietary.**

Trade secrets or other proprietary data contained in the proposal documents shall be maintained as confidential in accordance with procedures promulgated by the Procurement Officer and subject to limitations in Arizona or Federal law. **Pricing information cannot be considered proprietary or confidential.** The University shall not be liable in any manner or in any amount for disclosing proprietary information if such information is not clearly so designated and conspicuously so labeled. The University shall likewise not be liable if it did not know or could not have reasonably known that such information was proprietary. **At no time will the entire proposal be considered proprietary and be kept confidential. If the entire proposal is marked as confidential and/or proprietary and no redacted copy is sent, the University will not consider any part of the proposal confidential.**

3.9 EVALUATION PROCESS AND AWARD

3.9.1 Contractual Intent / Right to Terminate and Recommence RFP Process. The University intends to contract with one or more vendors whose proposal(s) are considered to be in the best interests of the University. However, the University may terminate this RFP process at any time up to notice of award, without prior notice, and without liability of any kind or amount. Further, the University reserves the right to commence one or more subsequent RFP processes seeking the same or similar products or services covered hereunder.

3.9.2 Effective Period of Proposals. Under this RFP, the University shall hold that vendors' responses to this RFP shall remain in effect for a period of ninety (90) days following the Due date, in order to allow time for evaluation, approval, and award of the contract. Any vendor who does not agree to this condition shall specifically communicate in its proposal such disagreement to the University, along with any proposed alternatives.

The University may accept or reject such proposed alternatives without further notification or explanation.

3.9.3 Proposal Acceptance/Rejection. The University reserves the right to reject any or all proposals. Such rejection may be without prior notice and shall be without any liability of any kind or amount to the University. The University shall not accept any proposal that the University deems not to be in its best interests. The University shall reject proposals submitted after the Due date and time.

3.9.4 Errors and Omissions in Vendors Proposals. The University may accept or reject any vendor's proposal, in part or in its entirety, if such proposal contains errors, omissions, or other problematic information. The University may decide upon the materiality of such errors, omissions, or other problematic information.

3.9.5 Determination of and Information Concerning Vendor's Qualifications. The University reserves the right to determine whether a vendor has the ability, capacity, and resources necessary to perform in full any contract resulting from this RFP. The University may request from vendors information it deems necessary to evaluate such vendors' qualifications and capacities to deliver the products and/or services sought hereunder. The University may reject any vendor's proposal for which such information has been requested but which the vendor has not provided. Such information may include but is not limited to:

- Financial resources
- Personnel resources
- Physical resources
- Internal financial, operating, quality assurance, and other similar controls and policies
- Resumes of key executives, officers, and other personnel pertinent to the requirements of the RFP
- Customer references
- Disclosures of complaints or pending actions, legal or otherwise, against the vendor

3.9.6 Apparently Conflicting Information Obtained by Vendor. The University is under no obligation whatsoever to honor or observe any information that may apparently conflict with any provision herein, regardless of whether such information is obtained from any office, agent, or employee of the University. Such information shall not affect the vendor's risks or obligations under a contract resulting from this RFP.

3.9.7 Rejection of Vendor Counter-offers, Stipulations and Other Exceptions. Any vendor exception, stipulation, counter-offer, requirement, and/or other alternative term or condition shall be considered rejected unless specifically accepted in writing by the University and thereafter incorporated into any contract resulting from this RFP.

3.9.8 Method of Award. Each response to this RFP will be reviewed for its overall competence, compliance, format, and organization. Proposals which the University deems overly complex, disorganized, or difficult to evaluate may be rejected in accordance with [Section 3.7.10](#) of this RFP. The award shall be made to the responsive and responsible vendor whose proposal is determined to be the most advantageous to the University of Arizona, taking into consideration the following evaluation criteria listed in the relative descending order of importance. Pricing must be a criterion. However, the

University is under no obligation whatsoever to select, as most responsive the proposal that demonstrates the lowest pricing.

3.9.8.1 Limiting Criteria:

If a Proposal does not meet ALL of the listed Limiting Criteria, it will not be eligible for consideration.

- Solution must provide a combined native POS and native Ecommerce system
- Solution must be Software as a Service (SaaS)
- Solution must integrate with Oracle NetSuite ERP Version 2026.1
- Solution must provide POS and Ecommerce system with real-time NetSuite inventory sync.
- Solution must have API integration capabilities
- Solution must have the ability to operate offline
- Solution must function and integrate with RF-Smart
- Solution must maintain Payment Card Industry Data Security Standard (PCI-DSS) compliance

3.9.8.2 Evaluation Criteria

- End User Experience / Functionality / Accessibility
- Administrator Experience / High Priority Technical Requirements
- Scalability of Solution / Configuration & Integration
- Reporting & Analytics
- Security / Compliance
- Implementation
- Cost
- Architecture / Deployment
- Product/ Technical Support
- Vendor Experience References & Recommendations

The contract will consist of the University's RFP, the proposal with any and all revisions, award letter, and/or purchase order, and/or the signed agreement between the parties, as stated in that agreement.

3.9.9 Selection, Negotiation, Additional Information. Although the University reserves the right to negotiate with any vendor or vendors to arrive at its final decision and/or to request additional information or clarification on any matter included in the proposal, it also reserves the right to select the most responsive and responsible vendor or vendors without further discussion, negotiation, or prior notice. The University may presume that *any proposal is a best-and-final offer*.

3.9.10 Pre-Award Presentations. The University reserves the right to require presentations from the highest ranked vendors, in which they may be asked to provide information in addition to that provided in their proposals.

3.9.11 Pre-Award Negotiations. The University reserves the right to negotiate prior to award with the highest ranked vendors for purposes of addressing the matters set forth in the following list, which may not be exhaustive.

- Resolving minor differences and scrivener's errors
- Clarifying necessary details and responsibilities

- Emphasizing important issues and points
- Receiving assurances from vendors
- Obtaining the lowest and best pricing and/or revenue agreement

3.9.12 Notification of Non-Selection. The University reserves the right not to notify vendors whose RFP responses are not selected for further consideration or notice of award. If the University decides to notify such vendors in writing, it will send the notifications to the address indicated in each such vendor's proposal. Once the award has been finalized, a notice of award may be posted on our [website](#).

3.9.13 Vendor's Need to Use Proprietary Rights of the University. All information proprietary to the University and disclosed by the University to any vendor shall be held in confidence by the vendor and shall be used only for purposes of the vendor's performance under any contract resulting from this RFP.

3.9.14 Public Record. After the award and execution of a contract resulting from this RFP, vendors' proposals become public record and are available for review during the University's regular office hours. The University will, in good faith and to the extent allowed by law, honor any vendor information that is clearly designated and conspicuously labeled as proprietary, and the University agrees that the information is proprietary. If the vendor needs to submit proprietary information with the proposal, the vendor **shall ensure that it is enclosed in a separate file from the proposal and that it is clearly designated and conspicuously labeled as such. The file must also contain the reason(s) why the enclosed material is to be considered proprietary.** At no time shall the entire proposal be considered proprietary and be kept confidential. The University shall not be liable in any manner or in any amount for disclosing proprietary information if such information is not clearly so designated and conspicuously so labeled. The University shall likewise not be liable if it did not know or could not have reasonably known that such information was proprietary. **Pricing information cannot be considered proprietary or confidential.**

3.9.15 Certification. By signature on the "Proposal Certification" form included herein, the Vendor certifies that the submission of the proposal did not involve collusion or other anti-competitive practices. The Vendor has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with the submitted proposal. In addition, Vendor certifies whether or not any employee of the University has, or has a relative who has, a substantial interest in any Agreement that may result from this RFP. Vendor also certifies their status with regard to debarment, or suspension by any Federal entity.

Failure to provide a valid signature affirming the stipulations required by this clause shall result in the rejection of the submitted proposal and, if applicable, any resulting Agreement. Signing the certification with a false statement shall void the proposal and, if applicable, any resulting Agreement. Any resulting Agreement may be subject to legal remedies provided by law. Vendor agrees to promote and offer to the University only those services and/or materials as stated in and allowed for under resulting Agreement(s).

4.0 AGREEMENT TERMS AND CONDITIONS

The following are the Terms and Conditions that will become part of any Agreement consummated between the University and the Successful Vendor. **In the event of a conflict between any provisions contained in any of the documents governing this transaction, the**

following shall be the order of precedence: Supplemental Agreement; Request for Proposals; Proposal.

- 4.1 Actions of Successful Vendor.** The University is under no obligation whatsoever to be bound by the actions of any Successful Vendor with respect to third parties. The Successful Vendor is not a division or agent of the University.
- 4.2 Advertising.** The Successful Vendor shall not advertise or publish information concerning the Agreement without prior written consent of the University. The University shall not unreasonably withhold permission.
- 4.3 Americans with Disabilities Act and Rehabilitation Act. The Successful Vendor will comply with all applicable provisions of the Americans with Disabilities Act, the Rehabilitation Act, and all applicable federal regulations.**

All electronic and information technology and products and services to be used by University faculty/staff, students, program participants, or other University constituencies must be compliant with the Americans with Disabilities Act as amended and the Rehabilitation Act. Compliance means that a disabled person can acquire the same information, engage in the same interactions, and enjoy the same services as a nondisabled person, in an equally effective and integrated manner, with substantially equivalent ease of use.

4.3.1 Electronic and Information Technology. Any acquisition considered electronic and information technology (EIT) as defined by the Access Board at 36 CFR 1194.4 and in the FAR at 2.101 must comply with Section 508 (36 CFR Part 1194) and, for web-based applications, WCAG 2.0, Level AA Guidelines. In addition, the submission of a completed Voluntary Product Accessibility Template (VPAT) is required so the University of Arizona may ascertain conformance. Proposals or bids without a completed VPAT may be disqualified from competition. The UA Guide to the VPAT and the templates themselves are available to assist vendors in this process. See information at <http://itaccessibility.arizona.edu/guidelines/purchasing/vpat>.

EIT is information technology (IT) and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. EIT includes, but is not limited to:

- telecommunication products, such as telephones;
- information kiosks and transaction machines;
- World Wide Web sites;
- software;
- multimedia (including videotapes); and
- office equipment, such as copiers and fax machines.

The University of Arizona reserves the right to perform real-world testing of a product or service to validate vendor claims regarding Section 508 conformance. To facilitate testing, the vendor will, upon request, provide the University with access to the product being considered for purchase for a period of at least 30 calendar days.

4.3.2 Services and Products. An accessible *service or product* is one that can be used by as many people as possible, taking into account their physical, cognitive, emotional, and sensory differences.

Services provided include, but are not limited to:

- education and training;
- cultural and athletic events;
- vehicle rentals
- event space and lodging; and
- parking and transportation.

Products include, but are not limited to:

- office equipment;
- office and classroom furniture; and
- kiosks

4.4 Conflict of Interest. Pursuant to the provisions of Arizona Revised Statute § 38-511, the Arizona Board of Regents may, within three years after its execution, cancel the Agreement without penalty or further obligation if any person significantly involved in negotiating, drafting, securing or obtaining the Agreement for or on behalf of the Arizona Board of Regents becomes an employee in any capacity of any other party or a consultant to any other party with reference to the subject matter of the Agreement while the Agreement or any extension thereof is in effect.

4.5 Drug Free Workplace. The Successful Vendor agrees that in the performance of the Agreement, neither the Successful Vendor nor any employee of the Successful Vendor shall engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance in conducting any activity covered by the Agreement. The University reserves the right to request a copy of the Successful Vendor's Drug Free Workplace Policy. The Successful Vendor further agrees to insert a provision similar to this statement in all subcontracts for services required.

4.6 Equal Opportunity. The provisions of Section 202 of Executive Order 11246.41 C.F.R. Sec. 60-1.4.41 C.F.R. Sec. 60-250.4 and 41 C.F.R. Sec. 60-741.4 are incorporated herein by reference and shall be applicable to the Agreement unless the Agreement is exempted under the rules, regulations or orders of the U.S. Secretary of Labor.

4.7 Federal, State, and Local Taxes, Licenses and Permits. Successful Vendor is solely responsible for complying with all laws, ordinances, and regulations on taxes, licenses and permits, as they may apply to any matter under this RFP. The Successful Vendor must demonstrate that they are duly licensed by whatever regulatory body may so require during the performance of the Agreement. Prior to the commencement of Agreement, the Successful Vendor shall be prepared to provide evidence of such licensing as may be requested by the University. Successful Vendor shall, at no expense to the University, procure and keep in force during the entire period of the Agreement all such permits and licenses.

4.8 Inspection and Audit. Pursuant to the provisions of Arizona Revised Statute § 35-214, all books, accounts, reports, files and other records relating to the Agreement shall be subject at all reasonable times to inspection and audit by the Arizona Board of Regents, The University of Arizona or the Auditor General of the State of Arizona, or their agents for five (5) years after completion or termination of the Agreement.

- 4.9 Liens.** Each Successful Vendor shall keep the University free and clear from all liens asserted by any person or entity for any reason arising out of the furnishing of services or materials by or to the Successful Vendor.
- 4.10 Modifications.** The Agreement can be modified or rescinded only by a writing signed by both parties or their duly authorized agents.
- 4.11 Non-Discrimination.** The parties shall comply with all applicable state and federal statutes and regulations governing equal employment opportunity, non-discrimination, and immigration.
- 4.12 Sales and Use Tax.** The Successful Vendor agrees to comply with and to require all of his subcontractors to comply with all the provisions of applicable law. The Successful Vendor further agrees to indemnify and hold harmless the University from any and all claims and demands made against it by virtue of the failure of the Successful Vendor or any subcontractors to comply with the provisions of any and all said laws. The University is not exempt from state sales and use tax, except for equipment purchased for research or development. Any equipment ordered as tax exempt shall be invoiced separately from taxable systems, even if purchased on the same purchase order as issued by the University.
- 4.13 Prohibited Harassment.** Federal law and the policies of the University prohibit sexual harassment of University employees or students. Sexual harassment includes any unwelcome sexual advance toward a University employee or student, any request for a sexual favor from a University employee or student, or any other verbal or physical conduct of a sexual nature that is so pervasive as to create a hostile or offensive working environment for University employees, or a hostile or offensive academic environment for University students. University vendors, subcontractors and suppliers for this project are required to exercise control over their employees so as to prohibit acts of sexual harassment of University employees and students. The employer of any person who the University, in its reasonable judgment, determines has committed an act of sexual harassment agrees as a term and condition of the Agreement to cause such person to be removed from the project site and from University premises and to take such other action as may be reasonably necessary to cause the sexual harassment to cease.
- 4.14 Small Business Utilization Program.** The University is committed to its [Small Business Utilization Program](#) and to the development of Small Business. If subcontracting is necessary, the Successful Vendor will make every effort to use Small Businesses in the performance of the Agreement.
- 4.15 Smoking and Tobacco Policy.** This policy applies to the University of Arizona main campus in Tucson, the Arizona Health Sciences Center, the Phoenix Biomedical Center, the College of Applied Science and Technology (UA South) and all University vehicles. This policy applies to University students, faculty, employees, contractors, volunteers, and visitors on its campuses and in its vehicles. To view the complete policy, click on <https://policy.arizona.edu/ethics-and-conduct/smoking-and-tobacco-policy>. The Successful Vendor is expected to respect this tobacco free policy and fully comply with it.
- 4.16 Export Control.** Each party shall comply with all applicable export control laws and economic sanctions programs. Applicable export control or economic sanctions programs may include U.S. export control laws such as the Export Administration Regulations and the International Traffic in Arms Regulations, and U.S. economic sanctions programs that are or may be maintained by the U.S. Government. The parties will comply with U.S. export

control and U.S. economic sanctions laws with respect to the export (including a deemed export) or re-export of U.S. origin goods, software, services and/or technical data, or the direct product thereof.

- 4.17 No Boycott of Goods or Services from Israel.** If the Goods/Services provided under this Agreement include the acquisition of services, supplies, information technology or construction with a value of at least \$100,000 and Supplier is engaged in for-profit activity and has 10 or more full-time employees, then, to the extent required by ARS § 35-393.01, Supplier certifies it is not currently engaged in, and during the term of this Agreement will not engage in, a boycott of goods or services from Israel.
- 4.18 No Forced Labor of Ethnic Uyghurs.** To the extent required by A.R.S. § 35-394, Successful Vendor certifies it is not currently, and during the term of this Agreement will not use: 1) the forced labor of ethnic Uyghurs in the People's Republic of China; 2) any goods or services produced by the forced labor of ethnic Uyghurs in the People's Republic of China; or 3) any contractors, subcontractors or suppliers that use the forced labor or any goods or services produced by the forced labor of the ethnic Uyghurs in the People's Republic of China. If the Successful Vendor becomes aware during the term of the awarded agreement that it is not in compliance with this written certification, it shall notify UArizona within five (5) business days of becoming aware of the non-compliance.
- 4.19 Safety Standards.** To the extent applicable to the services to be performed under this Agreement, Contractor represents and warrants that all articles and services furnished under this Agreement meet or exceed the safety standards established and promulgated under the Federal Occupational Safety and Health Law (Public Law 91-596) and its regulations, in effect or proposed as the date of this Agreement, which shall include the following guidance provided by OSHA, available at the following link <https://www.osha.gov/coronavirus/safework>. In addition, Contractor, Contractor employees, and/or subcontractors who will be performing work in University of Arizona locations, indoor or outdoor, must review and abide by the mask requirements listed at: <https://covid19.arizona.edu/face-coverings>.
- 4.20 Arbitration.** The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to ARS § 12-133.
- 4.21 Travel.** If authorized as part of any resulting contract, all reimbursable travel expenses must be authorized in writing by the University in advance of the planned travel and must be consistent with University Financial Policy 9.12 Independent Contractors, <https://policy.fso.arizona.edu/fsm/900/912> items 33-42. Each request for reimbursement shall be itemized and accompanied by copies of original receipts. If applicable, reimbursements for airfare shall be for standard airline coach travel only. If applicable, reimbursement for auto travel and per diem shall be made at the rate permitted for State of Arizona employees. Note that the purchase of alcohol shall not be permitted as a reimbursable expense under this Contract. Vendor will submit all receipts and any required backup documentation to the University within 90 days after the applicable expenses were incurred. The University will not be required to reimburse Vendor for any expenses, invoices, or receipts for expenses received after that time.
- 4.22 Administrative (Legal) Remedies.** The Arizona Board of Regents has promulgated [Administrative \(Legal\) Remedies](#) for alleged breaches or disputes arising from the Agreement. These remedies are exclusive and must be exhausted before the filing of any legal action.

- 4.23 Assignment-Delegation.** No right or interest in the Agreement shall be assigned or delegation of any obligation made by Successful Vendor without the written permission of the University. Any attempted assignment or delegation by Successful Vendor shall be wholly void and totally ineffective for all purposes unless made in conformity with this paragraph.
- 4.24 Assignment of Anti-Trust Overcharge Claims.** The parties recognize that in actual economic practice overcharges resulting from anti-trust violations are in fact borne by the ultimate purchaser; therefore, Successful Vendor hereby assigns to the University any and all claims for such overcharges.
- 4.25 Date for Reckoning Prompt-Payment Discount.** For purposes of determining whether a prompt-payment discount, if applicable, may be taken by the University, the starting date of such reckoning period shall be the later of the date of a properly executed invoice or the date of completion of service and/or delivery of product.
- 4.26 Force Majeure.** Neither party shall be held responsible for any losses resulting if the fulfillment of any terms or provisions of the Agreement are delayed or prevented by any cause not within the control of the party whose performance is interfered with, and which by the exercise of reasonable diligence, said party is unable to prevent. Neither the Supplier / Contractor nor the University shall be liable for failure to perform if such failure is caused by or due to acts or regulations of public authorities, labor difficulties, civil tumult, strike, epidemic, pandemic, or any cause beyond the control of Supplier / Contractor or the University. Neither party shall be under any further obligation to the other.
- 4.27 Indemnification / Hold Harmless.** The Successful Vendor shall indemnify, defend, and hold harmless to the fullest extent allowed by law the State of Arizona, the Arizona Board of Regents and the University, its officers, agents, and employees (“Indemnitees”) from any and all claims, demands, suits, actions, proceedings, loss, cost, and damages of every kind and description, including attorneys’ fees and/or litigation expenses, which may be brought or made against or incurred on account of breach, or loss of or damage to any property, or for injuries to or death of any person, or financial loss incurred by Indemnitees, caused by, arising out of, or contributed to, in whole or in part, by reasons of any act, omission, professional error, fault, mistake, or negligence of Successful Vendor, its employees, agents, representatives, or subcontractors, their employees, agents, or representatives in connection with or incident to the performance of the Agreement, or arising out of Workers Compensation claims, Unemployment Compensation claims, or Unemployment Disability Compensation claims of employees of Successful Vendor and/or its subcontractors of claims under similar such laws and obligations. Successful Vendor’s obligation under this provision shall not extend to any liability caused by the sole negligence of the State of Arizona, Arizona Board of Regents, University or its officers, agents, and employees. Such indemnification shall specifically include infringement claims made against any and all intellectual property supplied by Successful Vendor and third party infringement under the Agreement.
- 4.28 Indemnification by the University.** Arizona Revised Statute § 35-154 prohibits persons from incurring obligations against the state for which funds have not been appropriated or allocated. Arizona Attorney General’s Opinion 67-36-L interprets this statute to prohibit the state and its agencies from agreeing to hold harmless or indemnify third parties. The University shall be liable for claims, damages or suits arising from the acts, omissions or negligence of its officers, agents and employees.

4.29 Insurance Requirements. Without limiting any liabilities or any other obligations of Successful Vendor, the Successful Vendor shall provide and maintain the minimum insurance coverage listed below unless otherwise agreed to in writing. Coverage shall be provided with forms and insurers acceptable to the University until all obligations under the Agreement are satisfied.

- **Commercial General Liability (CGL)** insurance with minimum limits of ONE MILLION DOLLARS (\$1,000,000) each occurrence and TWO MILLION DOLLARS (\$2,000,000) general aggregate.
- **Commercial Automobile Liability** insurance with a minimum combined single limit of ONE MILLION DOLLARS (\$1,000,000) each occurrence.

The insurance policies required in the two statements above shall be endorsed to name the State of Arizona, Arizona Board of Regents on behalf of the University of Arizona as additional insured and shall stipulate that the insurance afforded the Successful Vendor shall be primary insurance and that any insurance carried by the State of Arizona, the Arizona Board of Regents and the University of Arizona, their agents, officials or employees shall be excess and not contributory insurance to that provided by Successful Vendor.

- If applicable, Worker's Compensation insurance in accordance with applicable Arizona Statutes, for any employees engaged in the performance of Agreement; and
- Employer's Liability insurance with a minimum limit of FIVE HUNDRED THOUSAND DOLLARS (\$500,000).

A certificate of insurance acceptable to the University shall be furnished to the University prior to the commencement of Agreement as evidence that policies providing the required coverage, conditions and limits are in full force and effect.

Technology/Network Errors and Omissions Insurance.

- Each Claim \$2,000,000
- Annual Aggregate \$4,000,000

a. This insurance shall cover Contractor's liability for acts, errors and omissions arising out of Contractor's operations or services, including loss arising from unauthorized access, or use that results in identity theft or fraud.

b. If the liability insurance required by the Agreement is written on a claims-made basis, Contractor warrants that any retroactive date under the policy will precede the effective date of the Agreement, and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of 2 years beginning at the time work under the Agreement is completed.

c. Policy shall cover professional misconduct for those positions defined in the scope of work of the Agreement.

4.30 Additional Insurance Requirements (Consultants, Lawyers, Architects and Engineers Agreements). In addition to the minimum insurance coverage and endorsement requirements stated in the paragraphs above, the Successful Vendor shall provide and maintain the minimum insurance coverage listed below unless otherwise agreed to in writing:

- **Professional Liability/Errors and Omissions** insurance with minimum limits of ONE MILLION DOLLARS (\$1,000,000) each claim and ONE MILLION DOLLARS (\$1,000,000) annual aggregate.

A certificate of insurance acceptable to the University shall be furnished to the University prior to the commencement of Agreement as evidence that policies providing the required coverage, conditions and limits as stated within this paragraph and the above paragraphs are in full force and effect.

- 4.31 Additional Insurance Requirements (Medical Services Agreement).** Not Applicable
- 4.32 Additional Insurance Requirements (Handling Hazardous Wastes).** Not Applicable
- 4.33 Intellectual Property.** It is understood and agreed that ownership of intellectual property developed as a result of fulfilling the requirements of this Request for Proposals belongs solely and exclusively to the Arizona Board of Regents on behalf of the University of Arizona. Documents/drawings used in this proposal belong to the Arizona Board of Regents on behalf of the University of Arizona and/or are being used with permission. Intellectual property as used herein, means all forms of legally protectable intellectual property, including copyrights, trademarks, inventions, patent applications, patents and mask works, drawings and/or blueprints. It is also understood and agreed that anything created as a result of an award of this proposal is considered a work for hire under the U.S. copyright laws and as such, the Arizona Board of Regents on behalf of the University of Arizona will own the copyright.
- 4.34 Labor Disputes.** Successful Vendor shall give prompt notice to the University of any actual or potential labor dispute which delays or may delay performance of the Agreement.
- 4.35 Laws and Regulations.** Successful Vendors are solely responsible for keeping themselves fully informed of and faithfully observing all laws, ordinances, and regulations affecting the rights of their employees, and shall protect and indemnify the University, its officers and agents against any claims of liability arising from or based on any violation thereof.
- 4.36 No Waiver of Right by the University.** No waiver by University of any breach of the provisions of the Agreement by the Successful Vendor shall in any way be construed to be a waiver of any future breach or bar the University's right to insist on strict performance of the provisions of the Agreement
- 4.37 Parking.** The Successful Vendor shall obtain all parking permits and/or decals that may be required while performing project work on University premises. The Successful Vendor should contact [Parking and Transportation Services](#) located at 1117 E. Sixth St., Tucson AZ 85721-0181.
- 4.38 Performance and / or Payment Bonds.** Intentionally Omitted
- 4.39 Payment Terms.** Payments by the University shall be subject to the provision of Title 35 of Arizona Revised Statutes relating to time and manner of submission of claims. The University's obligation is payable only and solely from funds appropriated for the purpose of the Agreement. Unless otherwise stated herein, the payment terms for the Agreement are Net 30 days
- 4.40 Price Adjustment for Multi-Year Contracts.** Price changes will normally only be considered at the end of one Agreement period and the beginning of another. Price change requests shall be in writing, submitted at least sixty (60) days prior to the end of

the current Agreement period, and shall be supported by written evidence of increased costs to the Successful Vendor. The University will not approve unsupported price increases that will merely increase the gross profitability of the Successful Vendor at the expense of the University. Price change requests shall be a factor in the Agreement extension review process. The University shall, in its sole opinion, determine whether the requested price increase or an alternate option is in the best interest of the University.

4.41 Prior Course of Dealings. No trade usage, prior course of dealing, or course of performance under other agreements shall be a part of any agreement resulting from this RFP; nor shall such trade usage, prior course of dealing, or course of performance be used in the interpretation or construction of such resulting agreement.

4.42 Referencing of Orders. For each order issued against an agreement resulting hereunder, the University intends in good faith to reference this RFP for pricing, terms and conditions, delivery location, and other particulars. However, in the event the University fails to do so, the University's right to such terms, conditions, and particulars shall not be affected, and no liability of any kind or amount shall accrue to the University.

4.43 Remedies and Applicable Law. The Agreement shall be governed by and construed in accordance with the laws of the State of Arizona. University and Successful Vendor shall have all remedies afforded each by said law. The venue in any action or litigation commenced to enforce the Agreement shall be instituted in the appropriate courts in Arizona.

4.44 Right of Assurance. Whenever one party to the Agreement in good faith has reason to question the other party's intent to perform, he may demand that the other party give a written assurance of their intent to perform. In the event that a demand is made and no written assurance is given within ten calendar (10) days, the demanding party may treat this failure as an anticipatory repudiation of the Agreement.

4.45 Right of Offset. The University shall be entitled to offset against any sums due the Successful Vendor, any expenses or costs incurred by the University, or damages assessed by the University concerning the Successful Vendor's non-conforming performance or failure to perform the Agreement, or any other debt owing the University, including expenses, costs and damages described in the termination provisions contained herein.

4.46 Termination

4.46.1 Convenience. The University reserves the right to terminate the Agreement in whole or in part at any time when in the best interests of the University without penalty or recourse. Upon receipt of the written notice, the Successful Vendor shall immediately stop all work as directed in the notice, notify all subcontractors of the effective date of the termination and minimize all further costs to the University. In the event of termination under this provision, all documents, data and reports prepared by the Successful Vendor under the Agreement shall become the property of and delivered to the University. The Successful Vendor shall be entitled to receive just and equitable compensation for work in progress, work completed and materials accepted before the effective date of termination. Such compensation shall be the Successful Vendor's sole remedy against the University in the event of termination under this provision.

- 4.46.2 Cause.** The resulting agreement may be terminated by either party for cause in the event of: (a) breach by the other party of a material obligation under the Agreement which is not remedied within thirty (30) days after written notice.
- 4.46.3 Suspension or Debarment.** The University may by written notice to the Successful Vendor immediately terminate the Agreement if the University determines that the Successful Vendor has been debarred, suspended or otherwise lawfully prohibited from participating in any public procurement activity, including but not limited to, being disapproved as a subcontractor Vendor of any public procurement unit or other governmental body.
- 4.46.4 Default.** The University reserves the right to terminate the Agreement in whole or in part due to the failure of the Successful Vendor to comply with any term or condition of the Agreement, to acquire and maintain all required insurance policies, bonds, licenses and permits, or to make satisfactory progress in performing the Agreement. The University shall provide written notice of the termination and the reasons for it to the Successful Vendor. Upon termination under this provision, all goods, materials, documents, data and reports prepared by the Successful Vendor under the Agreement shall become the property of and be delivered to the University on demand. The University may, upon termination of the Agreement, procure, on terms and in the manner that it deems appropriate, materials or services to replace those under the Agreement. The Successful Vendor shall be liable to the University for any Excess Costs incurred by the University in re-procuring the materials or services.
- 4.46.5 Gratuities.** The University may, by written notice to the Successful Vendor, cancel the Agreement if it is discovered by the University that gratuities, in the form of entertainment, gifts or other, were offered or given by the Successful Vendor, or any agent or representative of the Successful Vendor, to any officer or employee of the University with a view toward securing an Agreement or securing favorable treatment with respect to the awarding or amending, or the making of any determinations with respect to the performing of such Agreement. In the event the Agreement is canceled by the University pursuant to this provision, University shall be entitled, in addition to any other rights and remedies, to recover or withhold the amount of the cost incurred by Successful Vendor in providing such gratuities.
- 4.46.6 Insolvency.** The University shall have the right to terminate the Agreement at any time in the event Successful Vendor files a petition in bankruptcy; or is adjudicated bankrupt; or if a petition in bankruptcy is filed against Successful Vendor and not discharged within thirty (30) days; or if Successful Vendor becomes insolvent or makes an assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law; or if a receiver is appointed for Successful Vendor or its business.
- 4.46.7 Lack of Funding.** The Agreement may be canceled without further obligation on the part of the Arizona Board of Regents and the University of Arizona in the event that sufficient appropriated funding is unavailable to assure full performance of the terms. The Successful Vendor shall be notified in writing of such non-appropriation as soon as reasonably possible. No penalty shall accrue to the Board or the University in the event this cancellation provision is exercised. This cancellation provision shall not be construed so as to permit the University

to terminate the Agreement in order to acquire similar equipment, material, supplies or services from another party.

4.46.8 Stop Work Order. The University may at any time, by written order to the Successful Vendor, require the Successful Vendor to stop all or any part of the work called for by the Agreement for a period of ninety (90) days after the order is delivered to the Successful Vendor, and for any further period to which the parties may agree. The order shall be specifically identified as a Stop Work Order issued under this provision. Upon receipt of the order, the Successful Vendor shall immediately comply with its terms and take all reasonable steps to minimize the incidence of costs allocable to the work covered by the order during the period of work stoppage. If a Stop Work Order issued under this provision is canceled or the period of the order or any extension expires, the Successful Vendor shall resume work. The University shall make an equitable adjustment in the delivery schedule or Agreement price, or both, and the Agreement shall be amended in writing accordingly.

4.47 Continuation of Performance through Termination. The Successful Vendor shall continue to perform, in accordance with the requirements of Agreement, up to the date of termination, as directed in the termination notice.

4.48 Confidentiality. The parties shall comply with 20 USC Section 1232(g), the Buckley Amendment to the Family Educational Right and Privacy Act of 1974. Therefore, Vendor shall not be entitled to receive Employee or Student information directly from University, other than public information available in University directories which is not protected by federal or state privacy or confidentiality statutes or regulations. Vendor may solicit Employee and Student information directly from Employees and Students subject to prior disclosures by Vendor of all intended uses of such information. Regardless of the Employee or Student personal information, even if such information is publicly available via directories, Vendor shall under no circumstances sell, duplicate, market, or give to any person or persons, entities or other companies a list or other personal information of any or all Employees or Students. All identities and personal information Employees and Students shall remain confidential. And disclosure by Vendor occurring without the express prior written consent of the Employee or Student shall result in the immediate termination of this agreement.

4.49 Data Use, Ownership, and Privacy. As between the parties, UA will own, or retain all of its rights in, all data and information that UA provides to Supplier, as well as all data and information managed by Supplier on behalf of UA, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to the Agreement, even if generated by Supplier, as well as all data obtained or extracted through UA's or Supplier's use of such data or information (collectively, UA Data). UA Data also includes all data and information provided directly to Supplier by UA students and employees, and includes personal data, metadata, and user content.

UA Data will be UA's Intellectual Property and Supplier will treat it as UA Confidential Information (as defined below). Supplier will not use, access, disclose, or license, or provide to third parties, any UA Data, except: (i) to fulfill Supplier's obligations to UA hereunder; or (ii) as authorized in writing by UA. Without limitation, Supplier will not use any UA Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, UA's prior written consent. Supplier will not, directly or indirectly: (x) attempt to re-

identify or de- aggregate de-identified or aggregated information; or (y) transfer de-identified and aggregated information to any third party unless that third party agrees not to attempt re-identification or de-aggregation. For UA Data to be considered de-identified, all direct and indirect personal identifiers must be removed, including names, ID numbers, dates of birth, demographic information, location information, and school information. Upon request by UA, Supplier will deliver, destroy, and/or make available to UA, any or all UA Data.

Notwithstanding the foregoing, if the Agreement allows Supplier to provide aggregated and de-identified data to third parties, then Supplier may provide such data solely to the extent allowed in the Agreement, and, unless otherwise stated herein, only if such data is aggregated with similar data of others (i.e. is not identified as UA, ABOR, or Arizona-specific).

- 4.50 Non-Discrimination, Affirmative Action.** Contractor and subcontractor shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability.
- 4.51 Clean Air and Federal Water Pollution Control Act.** The successful vendor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C.1251–1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).
- 4.52 COVID-19 Safety Protocols.** The successful vendor must comply with FAR 52.223-99.
- 4.53 PCI DSS AND PABP COMPLIANCE.** Contractor acknowledges, warrants and will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data and/or sensitive authentication data and/or can affect security of those entities that store, process, or transmit cardholder data (e.g. Managed Services).

Furthermore, Contractor must certify at time of contract/agreement to be in compliance and continue to meet all applicable requirements by providing validation either by appearing on the VISA Global Registry of Service Providers (CISP), Payment Card Industry Security Standards Council Validated Payment Applications list (if applicable), or provide a completed and signed Attestation of Compliance (AOC) signed by a PCI approved Quality Security Assessor (QSA). Any change in Contractor’s certification requires prompt (within thirty (30) days) written notification to the University of Arizona.

Furthermore, Contractor agrees to provide to the University of Arizona upon request, any supporting compliance documentation such as but not limited to Approved Scan Vendor (ASV) Attestation of Compliance (AOC), external scan results, penetration testing results, and/or a completed Service Provider Self-Assessment Questionnaire (SAQ) D (if not completing a third-party assessment).

Contractor agrees to indemnify the University of Arizona for any breach of its cardholder data attributed to the application, system, or Contractor controlled interface to CHD or service provided by the Contractor. Contractor agrees to notify the University of Arizona authorized representative within 24 hours in the event of unauthorized release of cardholder data

Contractor must provide written documentation, which outlines the specific PCI DSS compliance responsibilities of both the Contractor and the University of Arizona.

4.54 Assignment. Contractor agrees that all copyrightable material, notes, records, drawings, designs, inventions, improvements, developments, discoveries, trade secrets and other work product that is conceived, made or discovered by Contractor, solely or in collaboration with others, during the performance of this Agreement, including all copyrights, patents, or other intellectual property rights therein (collectively, "**Work Product**"), are the sole property of the University. To the extent allowable under law, all Work Product will be deemed "Work For Hire" under the Copyright Act. To the extent any Work Product is not "Work For Hire," Contractor will assign (or cause to be assigned) and does hereby assign fully to University all right, title and interest in and to all Work Product. Contractor will assist University or its designee, at University's expense, in every proper way to establish, secure, perfect and maintain University's ownership rights in the Work Product, including the disclosure to the University of all pertinent information and data with respect thereto, and the execution of all applications, assignments and all other instruments reasonably requested by University.

4.55 Pre-Existing Materials. If, in the course of performing the Services, Contractor incorporates into any Work Product developed hereunder any invention, improvement, development, concept, discovery or other proprietary information owned by Contractor or in which Contractor has an interest: (i) Contractor shall inform University, in writing before incorporating such invention, improvement, development, concept, discovery or other proprietary information into any Work Product; and (ii) Contractor hereby grants University, under all of Contractor rights therein, a nonexclusive, royalty-free, perpetual, irrevocable, worldwide license to use, reproduce, distribute, perform, display, prepare derivative works of, make, have made, sell and export such item as part of or in connection with such Work Product. Developer shall not incorporate any invention, improvement, development, concept, discovery or other proprietary information owned by any third party into any Work Product without University's prior written permission.

4.56 Information Security Information Security and Privacy

4.56.1 Definitions Capitalized terms used but not defined in this section have the same meanings as set out in the Agreement.

Cloud Software means any externally hosted technology offering which enables on-demand Network access to a shared pool of configurable computing resources.

EEA means the European Economic Area (including the United Kingdom).

Medical Records means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers.

Network means any University network to which Vendor is provided access in connection with the performance of Services under the Agreement and/or any Vendor network that may access University Data.

Process or Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, device, or household.

Security Incident means any accidental, attempted, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, modification, disposal, compromise, or access to University Data or any act or omission that compromises or undermines the physical, technical, or administrative safeguards put in place by Vendor in Processing University Data or otherwise performing the Services.

System means any desktop or laptop, mobile device, server and/or storage device that, (i) is involved in the performance of the Services, (ii) may be used to access a Network, or (iii) may access or store University Data.

University Data means any and all data, information, text, graphics, works, and other materials that are collected, loaded, stored, accessible, transferred through and/or accessed by Vendor or provided to Vendor by University. This includes University's Systems and Network and also includes, but is not limited to: (1) all of the deliverables, reports, or materials from the Services; (2) all University information and materials that Vendor develops or acquires prior to, or independently of, the Agreement; (3) and any Personal Information or Medical Records pertaining to University end users, students, staff, patients or any other individuals identified in materials provided to or made accessible to Vendor by University. University Data is Confidential Information.

4.56.2 Restrictions on University Data Use

4.56.2.1 Vendor represents and warrants that it will only collect, access, use, maintain, and Process University Data for the sole and exclusive purpose of providing the Services in the Agreement, and may not retain, collect, use or disclose the University Data for any purpose other than performing the Services. Vendor may not share or sell the University Data for any reason or disclose the University Data to any third party except to provide the Services specified in the Agreement.

4.56.2.2 Upon termination or expiration of the Agreement or upon written request from University, whichever comes first, Vendor will, and will ensure that its Representatives (as defined below), immediately cease all use of and return to University or, at the direction of University, destroy all such University Data provided under this Agreement. If University elects for destruction, Vendor must certify to University that such University Data has been destroyed. If Vendor is required by law to retain any University

Data, Vendor must notify University of such requirement and will maintain the confidentiality of such University Data and may not use University Data for any purpose other than as required by law.

- 4.56.2.3** Vendor will limit access to University Data to its employees, contractors, subcontractors, and/or agents (“Representatives”) whose access is necessary to carry out the Services and will ensure those Representatives to keep all University Data confidential. Vendor will inform all Representatives of the confidential nature of University Data and all Representatives will be bound by confidentiality agreements with similar or greater confidentiality and security obligations as Vendor provides to University in the Agreement. Vendor agrees to be legally and financially liable for any breach of this Agreement, or unauthorized disclosure or misuse of University Data by its Representatives. The access rights of any Representatives will be removed immediately by Vendor upon termination or adjusted when such access is no longer necessary. Unless expressly consented to by University, Vendor will host and only allow access to University Data in the United States.
- 4.56.2.4** If Vendor and its Representatives will have access to University Data, Systems, or Networks, Vendor must ensure that its Representatives have undergone annual privacy and security training and adhere to Vendor’s policies and procedures that relate to privacy and security.
- 4.56.2.5** If Vendor is contacted by a third party with a request, inquiry, or complaint regarding University Data, Vendor will promptly (a) and in any event within two (2) calendar days, provide University with written notice of such request, inquiry or complaint to security@arizona.edu; and (b) provide University all reasonable cooperation, assistance, information and access to such data in its possession or control as is necessary for University to respond to such request, inquiry or complaint. Vendor will not respond to such request, inquiry or complaint unless so instructed in writing by University.

4.56.3 Written Information Security Program

- 4.56.3.1** At all times during the term of the Agreement, Vendor will implement and maintain a written information security program (“WISP”), which must include appropriate administrative, technical, physical, and operational safeguards to maintain the security, privacy, availability, integrity, and confidentiality of University Data in use, in motion, and at rest.
- 4.56.3.2** Vendor will implement and maintain a formalized risk governance plan, policy, and a continuous risk assessment process demonstrating Vendor’s ability to identify, quantify, prioritize, and mitigate risks. If requested by University, Vendor will (and/or cause subcontractors to) certify its compliance with the requirements of this Agreement and provide written responses to any reasonable questions submitted to Vendor by University. Vendor agrees to conduct and provide to University a Data Protection Impact Assessment (“DPIA”) or an independent audit report, if reasonably requested by University.

4.56.4 Data Privacy and Security

4.56.4.1 Vendor agrees to implement and maintain administrative, technical, physical, and operational safeguards in accordance with industry best practices at a level sufficient to secure University Data.

4.56.4.2 Vendor agrees to maintain the following enterprise controls for any Networks or Systems that host, Process, or provide access to University Data:

Asset and Information Management. Vendor will maintain and enforce policies and controls that include, without limitation, asset inventory/management, encryption (in transit and at rest), storage of data on portable hardware, and third-party access to and use of University Data.

Human Resources Security. Vendor will maintain and enforce a policy that addresses human resources security for all Representatives accessing University Data. Vendor will conduct background checks and not utilize any individual to fulfill the obligations of this Agreement if such individual has been convicted of any crime involving dishonesty or false statement including, but not limited to fraud and theft, or otherwise convicted of any offense for which incarceration for a minimum of one (1) year is an authorized penalty. Any such individual may not be a "Representative" under this Agreement.

Physical Security. All facilities used by or on behalf of Vendor to store and process University Data will implement and maintain administrative, physical, technical, and procedural safeguards in accordance with industry best practices at a level sufficient to secure University Data from a Security Incident. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event, less than reasonable in view of the type and nature of the data involved.

4.56.5 Data and System Access Controls. Vendor will maintain and enforce policies and controls that include, without limitation, role-based permissions for access to University Data (using a principle of minimization), restrictions on copying or removing data from an authorized network or system, strong password protocols (i.e., complexity requirements, mandatory changes, restrictions on sharing, etc.), and multi-factor authentication or equivalent protections for any remote access to Vendor's network or systems. Vendor will trace approved access to ensure proper usage and accountability, and the Vendor will make such information available to the University for review, upon the University's request and not later than five (5) business days after the request is made in writing.

4.56.6 Availability Control. Vendor will take industry-standard steps to ensure that University Data is available when requested by University. Additionally, Vendor must take steps to protect against accidental destruction or loss of University Data, including, without limitation, anti-virus software; firewalls; network segmentation; user of content filter/proxies; interruption-free power supply; threat detection and prevention; regular generation of and testing of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; business continuity and emergency plans; and air-conditioned server rooms.

4.56.7 Network Security. Vendor will carry out updates and patch management for all systems and devices in a timely manner, applying security patches within five (5) business days or less based on reported criticality. Updates and patch

management must be deployed using an auditable process that can be reviewed by the University upon the University's request and not later than five (5) business days after the request is made in writing. An initial report of patch status must be provided to the University prior to the effective date of the Agreement. Vendor will maintain documented operating procedures and technological controls to ensure the effective management, operation, and security, of Vendor's Network, including, without limitation, an up-to-date Network diagram, wireless encryption protocols, and adequate remote access protocols.

4.56.8 Logging and Monitoring. Vendor will comply with relevant security best practices for the monitoring and logging of its Networks, applications, and Systems. Logs will be kept for the duration of the Agreement or Vendor's record retention policy, whichever is longer.

4.56.9 Change Management and Web Applications. Vendor will use secure development and coding standards in accordance with industry standards. Vendor's web applications must meet OWASP Application Security Verification Standards (ASVS). Vendor will perform adequate testing prior to releasing updates, modifications, or new functionality to software.

4.56.10 Representations and Warranties. Vendor represents and warrants that: (i) it will comply with the requirements under applicable privacy and data security laws (including, if applicable, the General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999), the Children's Online Privacy Protection Act (COPPA), and/or Payment Card Industry Data Security Standard (PCI DSS)), and applicable state privacy and security laws; (ii) it will comply with the requirements of this Agreement, and (iii) it will perform the Services in accordance with industry standards and in a professional and workmanlike manner. If the Agreement requires or permits Vendor to access, receive, or release any student records, then, for purposes of this Agreement only, University designates Vendor as a "school official" for University under FERPA, as that term is used in FERPA and its implementing regulations.

If Vendor is provided access to Medical Records, but the applicable information is not subject to HIPAA, Vendor represents and warrants that it will (i) comply with 16 C.F.R, Part 318 and (ii) only use or disclose Medical Records as permitted or required under the Agreement, or as required by law. At all times during the course of the Agreement, Vendor will make any Medical Records available to University for access, portability, modification, or deletion.

Vendor represents and warrants that all responses to any security assessment by University are accurate and truthfully represents the security practices of Vendor. Vendor agrees that, at the request of University, it will provide sufficient evidence of its compliance with obligations set forth in this Agreement.

4.56.11 Data Security Incident. Vendor will maintain, update and document an Incident Response Plan ("IRP"), and will manage, document, review, investigate and resolve all Security Incidents in accordance with the IRP.

Vendor agrees to notify University of a Security Incident at security@arizona.edu as soon as reasonably practicable and without undue delay. Such notice must

include (i) a description of the incident, including the type of incident (e.g., theft, loss, improper disclosure, unauthorized access), location of the incident (e.g., laptop, desktop, paper), how the incident occurred, the date the incident occurred, and the date the incident was discovered; (ii) a description of the type of University Data involved (e.g., user data, intellectual property, etc.); (iii) a description of the potentially impacted individuals; (iv) a description of the actions taken in response to the Security Incident (e.g., additional safeguards, mitigation, sanctions, policies, and procedures); and (v) all other information reasonably requested by University or necessary to provide notice to individuals and/or regulators, including a forensic report summarizing the findings of a forensic investigation. University acknowledges that certain information may not be immediately available and can be provided on a rolling basis as it is discovered (within 72 hours of discovery).

In facilitating the investigation and remediation of a Security Incident, Vendor will cooperate fully with University. Vendor may not inform any third party of any Security Incident without first obtaining the University's written consent, except as may be required by law. Vendor agrees to reimburse University for reasonable costs and expenses incurred (including legal fees) in responding to, remediating, and/or mitigating damages caused by a Security Incident or in following up on a complaint by an individual or a regulator. Vendor will take all necessary and appropriate corrective actions, including as may be reasonably instructed by University, to remedy or mitigate any Security Incident.

4.56.12 Audit and Testing Vendor will complete one of the following audits at least annually and immediately after any actual or reasonably suspected Security Incident: SOC 2 Type II, SOC for Cybersecurity, or an accepted Higher Education Cloud Vendor Assessment Tool (<https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit>). Evidence must be provided to the University prior to this Agreement and at least annually thereafter.

Prior to this Agreement, and at regular intervals of no less than annually and whenever a change is made which may impact the confidentiality, integrity, or availability of University Data, and in accordance with industry standards and best practices, Vendor will, at its expense, perform scans for unauthorized applications, services, code and system vulnerabilities on the Networks and Systems used to perform Services related to this Agreement ("Security Tests"). An initial report must be provided to the University prior to this Agreement. Vendor will provide the University the reports or other documentation resulting from the audits, certifications, scans and tests within five (5) business days of Vendor's generation or receipt of such results. If any critical finding is identified, Vendor agrees to notify the University and remediate the critical finding within thirty (30) days. Any critical finding not remediated within thirty (30) days must be reported to University at security@arizona.edu. All other findings must be remediated within ninety (90) days. At University's request, Vendor will promptly provide written attestation that required Security Tests, independent audits, and/or a DPIA have been conducted either by a qualified Representative or by a third party in the prior twelve (12) months. The University may require the Vendor to perform additional audits and tests, the results of which will be provided to the University within five (5) business days of the Vendor's receipt of such results.

Vendor agrees to take reasonable steps to assist University in maintaining the accuracy of such University Data under the control of Vendor, including synchronizing relevant Systems, databases, or applications, as deemed

necessary by University. The University reserves the right to, at a minimum, an annual, review of: Vendor's access reports related to access to University Data; Vendor's patch management process, schedules, and logs; findings of vulnerability scans and/or penetration tests of Vendor Systems; and Vendor development standards and processes.

4.56.13 International Transfers. If University provides its written consent for Vendor to transfer Personal Information from EEA countries to countries outside the EEA, the terms set out in the EU Standard Contractual Clauses will apply. The parties will work in good faith to populate appendices 1 and 2 of the EU Standard Contractual Clauses and attach an executed version to this Agreement. Vendor agrees to comply with all obligations imposed on a "data importer" set out in such EU Standard Contractual Clauses. For countries located within the Asia Pacific region, Vendor must obtain University prior written consent where Personal Information will be transmitted by the Vendor outside the country from which it was originally collected.

4.56.14 Use of Artificial Intelligence in Providing the Goods/Services

4.56.14.1 Definition of AI. As used herein, "Artificial Intelligence" or "AI" means technologies, including but not limited to machine learning, deep learning, and neural networks that are capable of performing tasks that typically require human intelligence, such as content generation, visual perception, speech recognition, decision-making, and language translation.

4.56.14.2 Compliance with Laws. The Supplier shall adhere to all current and applicable federal, state, and local laws and other regulatory requirements applicable to the development, deployment, and management of AI technologies utilized under this Agreement.

4.56.14.3 Subcontractors. Supplier shall ensure any of its subcontractors using AI services directly relating to the delivery of the Goods/Services (including any use of University data) complies with the same standards and obligations imposed on Supplier in this Agreement. Supplier will not share any University Data with any of its subcontractors for the purpose of training AI models without explicit written consent from the University detailing the scope and purpose of data usage.

4.56.14.4 Disclosure of AI Subcontractors. Upon request by the University, the Supplier shall provide a comprehensive list of all of its subcontractors engaged in providing AI services under this Agreement, including descriptions of their roles and involvement.

4.56.14.5 Prohibition on Use of University Data in AI Training. The Supplier is expressly prohibited from using any data provided by the University, including personal and sensitive data, to train or fine-tune AI models, except as follows:

The University may permit the use of non-personally identifiable information (non-PII) for training or fine-tuning purposes under strict conditions that safeguard the confidentiality and ownership of such data. Under no circumstances shall the Supplier repurpose any University Data, including text and non-PII, for the benefit of other clients or for any

use outside the scope explicitly approved by the University in writing. The University retains full ownership of its data, and the Supplier must not use, disclose, or allow access to the data for any purposes not specifically authorized by the University.

4.56.14.6 Consent Required for New AI Capabilities. Any new AI product capabilities proposed by the Supplier must either 1) receive prior written approval from the University before such capabilities are provided to or used by the university; or 2) the AI feature will be disabled by default and can only be enabled once the University has received at least thirty (30) days' prior written notice of the new AI product capabilities being implemented. The university retains the right to review such capabilities to assess their impact on operations and data security.

4.56.14.7 Data Protection and Security Measures. Supplier must implement stringent data protection and security measures that comply with applicable laws and industry standards to protect University data from unauthorized access or breaches.

4.56.14.8 Appendices

4.56.14.8.1 If Vendor is a Cloud Software provider, then the Cloud Software Appendix (section 6.5) will apply.

4.56.14.8.2 If Vendor is processing credit or debit card transactions on behalf of University, the PCI Appendix (Section 6.6) will apply.

4.56.14.8.3 If Vendor is collecting, accessing, acquiring, or otherwise Processing Protected Health Information (as defined in the Health Insurance Portability and Accountability Act of 1996), then the PHI Appendix/Business Associate Agreement (Section 6.7) will apply.

4.56.15 Survivability. Vendor's obligations under this section (Information Security) of the Agreement will survive the termination or expiration of the Agreement and will apply so long as Vendor may access or be in possession of University Data, Network, or Systems. Any requirements imposed on Vendor in this Agreement shall apply to any of Vendor's subcontractors. Following the termination of the Agreement for any reason, Vendor agrees to provide transition services for the benefit of University, including a month-to-month extension (not to exceed ninety (90) days) for the continued provision of its Services and reasonable assistance with the transfer of University Data. The parties agree to take such reasonable actions as are necessary to amend this Agreement from time to time as is necessary for the parties to comply with applicable privacy laws. In the event of inconsistency between the Agreement and this Information Security section, the Information Security Section will govern.

5.0 SCOPE OF WORK AND RESPONSE INSTRUCTIONS

Scope of Work:

The University will be replacing NetSuite POS and Suite Commerce and intend to find a solution that will eliminate data silos, enhance financial reconciliation, streamline operations during off-site events (e.g., Tucson Festival of Books), and reduce manual data entry.

Some of the pain points to be addressed are the returned merchandise process, lack of automated inventory and financial reports, and streamline marketing efforts for the e-commerce team. The new solution should support credit/debit, cash, and [CatCa\\$h](#) transactions.

Response Instructions:

1. Provide a brief company and solution overview that addresses how your offering meets our needs. Your narrative should be no longer than three (3) pages and should cover your company background, relevant experience serving clients with similar needs, solution overview, and key differentiators. The narrative is intended to give evaluators context and confidence in your organization, it is not a comprehensive technical response. Detailed responses to specific requirements should be provided in Attachment A as described below.
2. Responses to the detailed requirements and specifications should be provided in **Attachment A**. In order to be considered for award, your solution must meet the following minimum requirements as noted on the “Limiting Criteria” tab:
 - Solution must be a unified commerce SaaS solution that provides integrated Point of Sale (POS) and eCommerce capabilities within a single platform.
 - The solution must integrate with:
 - NetSuite ERP version 2026.1. This will remain the backend ERP system for General Merchandise (GM), Inventory Management, Financial (AP, AR), and Textbook and Course materials.
 - Inventory/Warehouse management (RF Smart). Inventory updates must occur in near real-time across all sales channels.
 - The solution must provide unified order management, allowing staff to view, manage, and report on orders from both POS and eCommerce within the same administrative interface.
 - The solution must support cross-channel returns and refunds including the ability to return or refund eCommerce purchases at a physical POS location.
 - The solution must be able to operate offline with cached local data for 24-48 hours. The solution should allow for notifications sent when solution is operating offline or goes offline.
 - The solution must maintain Payment Card Industry (PCI) data security standards.
 - Avalara tax software. This is required to reduce the manual process of calculating tax rates and should be based on location for more accurate calculations.
 -

5.1 Current State and Assumptions

5.1.1 The University Campus Store is a retail entity operating within an educational Institution. Because of this, the environment has complex integration requirements. The goal is to minimize the number of systems used to pull and run reports, tax data, E-commerce reports that include data from website visits and transactions

5.1.2 To give an idea of scope and scale, the University of Arizona has approximately \$2M in annual ecommerce online sales with approximately 157k online transactions. The annual POS sales are approximately \$13.781M with approximately 202k POS register transactions. The Campus Store has approximately 40 POS desktops/apps streaming software. The expectation is that usage will increase during the life of the contract.

5.2 End User Experience / Functionality / Accessibility

- 5.2.1 Our solution supports multiple POS and e-commerce users; such as student and hourly workers through flexible, role-based access controls, with configurable permissions and the ability to create custom roles as needed. The current browser-based system is used by POS users with limited training and minimal on-site technical support. The POS experience is designed to reduce complexity, enabling users to complete common workflows—such as scanning items, applying discounts, handling returns, and accepting multiple tenders—with minimal steps.
- 5.2.2 The University has alumni across the country and has established tax nexus in all 50 states; therefore, it is critical that the e-commerce solution accurately calculate and apply sales tax based on the customer’s shipping location and applicable state and local tax rules. The platform integrates with Avalara to perform real-time tax calculations during checkout, ensuring compliance with multi-state tax regulations and automatically applying the correct rates and product taxability rules for each jurisdiction. This integration also supports accurate reporting and audit-ready transaction records for tax filings.

5.3 Administrator Experience / High Priority Technical Requirements

- 5.3.1 The University’s system needs are: to meet enterprise integration, security, and operational requirements while remaining easy to manage with limited technical resources. It should support SSO via Shibboleth, native API-based integration while allowing Avalara tax software for real-time tax calculation, and certified integration with Oracle NetSuite using SuiteTalk REST APIs with Token-Based Authentication and a clear path to OAuth 2.0. The platform enforces TLS 1.2+ for all integrations, uses AES-256 encryption at rest, and follows strict role-based access controls, with SOC 2 Type II certification in place. Administrators have access to centralized dashboards for configuration, user management, and audit logging, with flexible user provisioning (manual, bulk import, LDAP/SCIM) and role-based access controls that support multiple roles per user.
- 5.3.2 Sandbox and staging environments are required for testing configurations, integrations, and updates, and the platform should follow a continuous release model with advance notification and minimal downtime. Operationally, POS registers should have the capability to be rapidly provisioned and configured for stores or temporary events, with the ability to add devices on demand using supported, non-proprietary hardware. Register configurations can be switched between locations with minimal effort and no advanced technical expertise required. The system provides transaction-level logging, monitoring, and replay capabilities across integrations (NetSuite, Watchman, RF-SMART, Hyperspace), ensuring full auditability and reliable financial reconciliation.

5.4 Scalability of Solution / Configuration & Integration

- 5.4.1 The solution should scale reliably with growth in transaction volume, users, locations and product catalog size, while maintaining strong performance during peak periods. The solution should offer flexible, well-documented integration capabilities (REST, APIs, web hooks, middleware, file-based methods) with robust support for real-time, bi-directional data exchange across our key enterprise system NetSuite and specialized integrations like Watchman, RF-Smart and device management tools. It must support automation, scheduling, and open API access with clear authentication and rate limit handling. Additionally, the platform should offer configuration & customization, and include performance optimizations like caching, CDN using and load balancing.

5.5 Architecture / Deployment

- 5.5.1** Currently, our solution supports 30 + simultaneous transactions on multiple active POS register sessions, at multiple sites, allowing transactions to occur concurrently without performance degradation. The POS architecture is designed to process transactions in real time while simultaneously updating inventory levels to ensure accurate stock availability across all registers and the e-commerce platform. Each register communicates with centralized cloud services through secure APIs, enabling immediate validation of pricing, promotions, and tax calculations while recording completed transactions.
- 5.5.2** To ensure smooth performance during periods of high activity, the platform leverages scalable cloud infrastructure hosted on Amazon Web Services, which automatically adjusts computing resources based on transaction volume. This architecture ensures sufficient bandwidth and processing capacity so that multiple registers can complete transactions simultaneously without lag. Inventory updates are processed through real-time integration with Oracle NetSuite, ensuring that product quantities are reduced immediately after each completed transaction and remain synchronized across POS and e-commerce channels.
- 5.5.3** In addition, each POS register maintains a locally cached dataset that includes product catalog data, pricing, promotions, and tax tables. This local caching enables fast transaction processing even during temporary network disruptions. Transactions completed while offline are securely queued and automatically synchronized with the central system once connectivity is restored, ensuring that no sales data or inventory updates are lost or duplicated.
- 5.5.4** We are currently contracted with Avalara tax software in order to reduce the manual process of calculating tax rates and should be based on location for more accurate calculations.

5.6 Reporting & Analytics

- 5.6.1** The solution should provide out-of-the-box reporting and analytical tools across POS and e-commerce with configurable dashboards to find and build reports. To use the dashboards to access real-time and historical reporting data for sales via POS and e-commerce. The University of Arizona currently uses Oracle NetSuite ERP for financial data and reporting.

5.7 Security & Compliance

- 5.7.1** The POS and eCommerce solution adheres to strong security and compliance standards across the full software development lifecycle, including secure coding practices, regular testing, and vulnerability management. The awarded solution must ensure robust protection of Personally Identifiable Information (PII) through encryption, access controls, and data governance policies, while enforcing secure API communications using TLS 1.2 or higher without fallback to deprecated protocols. Additionally, it should align with university-level security and risk management requirements, including support for PCI-DSS compliance, penetration testing, disaster recovery and rollback procedures, and continuous monitoring to maintain system integrity and data privacy across all integrated platforms.

5.8 Implementation

- 5.8.1** The university is looking for a partner that can guide us through a structured and well-managed implementation of a new POS and e-commerce solution. Based on what we've seen, a typical implementation for an institution our size would take approximately six to nine months, following a phased approach that includes discovery, design, configuration, integration, testing, and go-live support. It's important to us that the work is led by an experienced team, with the ability to leverage partners

when needed, and that a dedicated project manager is assigned to keep the effort organized, on track, and clearly communicated throughout.

5.9 Term of Agreement. The term of this agreement is expected to be an initial three (3) years with two (2) additional optional one-year extension that can be exercised annually.

5.10 Furnish and Install. The items specified in this solicitation will be provided on a furnished and installed basis. The Successful Vendor shall have the complete responsibility for the items or system until it is in place and working. Any special installation preparation and requirements must be submitted to the University as part of this proposal. All transportation and coordination arrangements will be the responsibility of the Successful Vendor. Delivery of equipment will be coordinated so that items or system will be delivered directly to the installation site. This effort will minimize risk of damage and avoid double handling.

Detailed Pricing. Please detail all pricing and fees on the Pricing tab of Attachment A.

5.11 Method of Payment & Discount for Early Payment. The University's preferred method of payment is via credit card. The University would issue a Purchase Order and upon receipt of goods or services, pay subsequent invoices by credit card.

Will you accept payment via credit card? Yes _____ No _____

Do you offer an early payment discount? Yes _____ No _____
If yes, what is your offer? _____ % if paid within _____ days after the University receives a proper, accurate and uncontested Invoice for Payment.

If payment via credit card is accepted and an early payment discount is offered, would the University receive the discount if paying by credit card? Yes _____ No _____

5.12 References. Vendor to provide two (2) customer references, from comparable institutions for similar products or services specified in this RFP, including the company names, contact names, telephone numbers and emails of the contact persons.

6.0 CERTIFICATIONS AND FORMS

Supplier to complete forms below and return with proposal

6.1 Certification of Proposal

6.2 Legal Workers Certification (Required for all Contracts for: Services; Construction or Maintenance of Structure, Building or Transportation Facility; or Improvements to Real Property costing \$100K and over)

6.3 Certification Regarding Debarment, Suspension, Proposed Debarment and other Responsibility Matters (Mar 1996 as amended) (Applicable to Federal Grants and Contracts >\$30k)

6.4 Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (Apr 1991 as amended) (Applicable to Federal Grants and Contracts >\$150k)

6.5 Cloud Software Appendix

6.6 PCI Appendix

6.7 PHI Appendix/Business Associate Agreement

6.1. Certification of Proposal (vendor to complete and return with proposal)

Explanation. This certification attests to the vendor’s awareness and agreement to the content of this RFP and all accompanying provisions contained herein.

Action. Vendor is to ensure that the following certificate is duly completed and correctly executed by an authorized officer of your company.

This proposal is submitted in response to Request for Proposals # [REDACTED] issued by the University of Arizona. The undersigned, as a duly authorized officer, hereby certifies that _____ (Vendor Name), located at _____ (address), agrees to be bound by the content of this proposal and agrees to comply with the terms, conditions and provisions of the referenced Request for Proposals (RFP) and any addenda thereto in the event of an award. Exceptions are to be noted as stated in the RFP. The proposal shall remain in effect for a period of ninety- (90) calendar days as of the Due Date for responses to the RFP.

The undersigned certifies that to the best of his/her knowledge: (check one)

There is no officer or employee of the University of Arizona who has, or whose relative has, a substantial interest in any Contract award subsequent to this proposal.

The names of any and all public officers or employees of the University of Arizona who have, or who's relative has, a substantial interest in any Contract award subsequent to this proposal are identified by name as part of this submittal.

The undersigned further certifies that their firm (check one) IS **or** IS NOT currently debarred, suspended, or proposed for debarment by any federal entity. The undersigned agrees to notify the University of any change in this status, should one occur, until such time as an award has been made under this procurement action.

In accordance with [Purchasing Policy 4.3](#) – Small Business Utilization Program, the Undersigned further certifies that your business (check the appropriate areas) does **or** does not meet the Federal (S.B.A.) Small Business definition (FAR 19.001) and size standards (FAR 19.102). If it does, please “CHECK” one of the following: Small Business Small Disadvantaged Small Business Women-Owned Women-Owned Disadvantaged Veteran owned HUB Zone Disabled Veteran Owned Alaska Native Corp. Historically Black Colleges and Universities and Minority Institutions

[Arizona Small Business](#) (has less than 100 fulltime employees, including employees employed in any subsidiary or affiliated corporation) please “CHECK one of the following: AZ. Small Business AZ. Women Owned AZ Disadvantaged AZ Disadvantaged Women-owned.

The undersigned further certifies that as a duly authorized officer, is authorized to negotiate in good faith on behalf of this firm for purposes of this Request for Proposals.

Name: _____ Title: _____

Signature: _____ Date: _____ Email: _____

F.E.I.N: _____

RFP Email and Notification Contact: _____

6.2. LEGAL WORKER CERTIFICATION

Required for all Contracts for: Services; Construction or Maintenance of any Structure, Building or Transportation Facility; or Improvements to Real Property costing \$100K and over.

Date: _____

Procurement and Contracting Services
University of Arizona
PO Box 210300
Tucson, AZ 85721-0300

As required by Arizona Revised Statutes §41-4401 the University is prohibited after September 30, 2008 from awarding a contract to any contractor who fails, or whose subcontractors fail, to comply with Arizona Revised Statutes § 23-214-A. The undersigned entity warrants that it complies fully with all federal immigration laws and regulations that relate to its employees, that it shall verify, through the employment verification pilot program as jointly administered by the U.S. Department of Homeland Security and the Social Security Administration or any of its successor programs, the employment eligibility of each employee hired after December 31, 2007, and that it shall require its subcontractors to provide the same warranties to the below entity.

The undersigned acknowledges that a breach of this warranty by the below entity or by any subcontractor(s) under any Contract resulting from this solicitation shall be deemed a material breach of the Contract and is grounds for penalties, including termination of the Contract by the University. The University retains the right to inspect the records of the below entity, subcontractor(s) and employee(s) who perform work under the Contract, and to conduct random verification of the employment records of the below entity and any subcontractor(s) who perform work under the Contract, to ensure that the below entity and each subcontractor is complying with the warranties set forth above. Contractor shall be responsible for all costs associated with compliance with such programs.

(Firm) _____
(Address)

(Signature Required)

(Phone)

(Print Name)

(Fax)

(Print Title)
Number)

(Federal Taxpayer ID

(November 3, 2009)

6.3. CERTIFICATION REGARDING DEBARMENT SUSPENSION, PROPOSED DEBARMENT AND OTHER RESPONSIBILITY MATTERS (MAR 1996)

In accordance with FAR 52.209.5, complete the following certification regarding debarment suspension, proposed debarment and other responsibility matters and **return the completed certification with your solicitation response.** (Applicable to Federal Contracts and Grants >\$30k)

(a) Certification Regarding Debarment Suspension, Proposed Debarment, and Other Responsibility Matters (Mar 1996 as amended)

- (1) The Offeror certifies, to the best of its knowledge and belief, that
 - (i) The Offeror and/or any of its Principals
 - (A) **Are** **Are Not** presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency,
 - (B) **Have** **Have Not** , within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract, violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and
 - (C) **Are** **Are Not** presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in subdivision (a)(1)(i)(B) of this provision.
 - (ii) The Offeror **Has** **Has Not** , within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.
 - (2) "Principals", for the purposes of this certification, means officers; directors, owners, partners; and, persons having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment and similar positions). This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.
- (b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
 - (c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.
 - (d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
 - (e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government the Contracting Officer may terminate the contract resulting from this solicitation for default. (End of Provision)

(NAME OF FIRM)

(ADDRESS, CITY, STATE, ZIP)

(SIGNATURE)

(DATE)

(PRINT OR TYPE - NAME AND TITLE)

6.4. CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (APR 1991 as amended)

In accordance with FAR 52.203-11 and FAR 52.203-12 entitled "Limitation on Payments to Influence Certain Federal Transactions (Jun 1997 as amended), the following certification and disclosure regarding these FAR provisions are hereby incorporated and made a part of this bid/proposal solicitation requirement. (Applicable to Federal Grants and Contracts >\$150k)

- (a) The definitions and prohibitions contained in the clause, at FAR 52.203.12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in paragraph (b) of this certification.
- (b) The Offeror, **by signing its offer**, hereby certifies to the best of his or her knowledge and belief that on or after December 23, 1989
 - (1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any Federal contract, grant, loan, or cooperative agreement;
 - (2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the Offeror shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the Contracting Officer; and
 - (3) He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of \$ 100,000 shall certify and disclose accordingly
- (c) Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by section 1352, title 31, United States Code. Any person who makes expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision, shall be subject to a civil penalty of not less than \$10,000, and not more than \$100,000, for each such failure.

(NAME OF FIRM)

(STREET ADDRESS)

(SIGNATURE)

(MAILING ADDRESS)

(TYPED OR PRINTED NAME)

(CITY, STATE, ZIP)

(DATE)

6.5. Cloud Software Appendix

In addition to the terms in the AGREEMENT, the following terms will apply if the Services provided under this Agreement are provided to University as Cloud Software.

1. **Vendor Obligations.** In addition to any other obligations of Vendor, Vendor must:
 - a) Provide the Services on a continuous basis and warrants that the Services will be fully available 99.9% of each month, except for scheduled maintenance for which written notice has been provided to University at least thirty (30) calendar days in advance.
 - b) Provide unlimited telephone support twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year (“24/7/365”).
 - c) Provide online access to technical support bulletins and other user support information and forums 24/7/365;
 - d) Conduct quarterly support updates and reviews involving technical teams from both Parties to discuss Cloud Software support issues.
 - e) Provide semi-annual support usage, incident reports and Vendor’s compliance with any service levels identified in a service level agreement.
 - f) Respond with support to Priority One Issues (as defined below) within one (1) hour of University’s call for assistance to Vendor and initiate work on such issues within one (1) hour thereafter, regardless of time of day or day of week. Priority One Issues include issues involving substantial failure of the Cloud Software, which, in University’s sole judgment, are critical to its operations. Vendor will initiate work on all other support issues, within four (4) hours from receipt of an electronic or telephonic service request.
 - g) In the event two or more Priority One Issues occur in any thirty (30) day period during the term of the Agreement, Vendor will promptly investigate the root causes of such support issues and will provide to University an analysis of such root causes and a proposed corrective action plan for University’s review, comment and approval (the “Corrective Action Plan”). The Corrective Action Plan must include, at a minimum: (i) a commitment by Vendor to University to devote the appropriate time, skilled personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of Priority One Issues; (ii) a strategy for developing any programming/software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of such issues; and (iii) time frames for implementation of the Corrective Action Plan. There will be no additional charge (other than those fees set forth in this Agreement) for Vendor’s implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan.
2. **Scheduled Maintenance of Cloud Software.** Scheduled maintenance, updates, enhancements or modifications relative to the Services and/or other elements or components of the Services will be in accordance with Vendor’s maintenance schedule and will not in any way diminish the benefits, comprehensiveness, features or functionality of the Services, as defined under the Agreement. Vendor may, however, push updates and fixes at any time to University that Vendor determines will not affect University’s ability to access the Services. Unless otherwise agreed in writing, non-peak hours are from Friday night at 11:00 p.m. MST through Saturday morning at 8:00 a.m. MST, and Saturday night at 11:00 p.m. MST through Sunday morning at 8:00 a.m. MST.
3. **Unscheduled Maintenance of Cloud Software.** If the Services provided under this Agreement are provided to University as Cloud Software, Vendor will provide University with at least seventy-two (72) hours prior notice of Vendor’s implementation of all unscheduled maintenance, updates, enhancements, modifications and/or other circumstances which will result in an outage or an inability of University to access the Services. In the event emergency maintenance of the Services is required, Vendor will provide University with as much advance notice as possible of the impending emergency maintenance and will disclose to University, in writing, the cause or issue necessitating the emergency maintenance as soon as possible and no later than seventy-two (72) hours after the initiation of the emergency maintenance.
4. **Critical Services Not to be Abandoned.** Vendor acknowledges that the Cloud Software provided under this Agreement are critical services for University. Accordingly, notwithstanding any other provisions under the Agreement to the contrary, the Parties agree that Vendor may not “**Abandon**” such critical Services. For purposes of an Agreement, “Abandon” means Vendor’s actual, willful non-performance of any material aspect of the Services in breach of the Agreement which results in a material adverse effect on (i) critical aspects of University’s internal

operations, regulatory or other reporting requirements; or (ii) a Service that is provided to or in support of University's students and faculty. Abandonment will not be deemed to have occurred if non-performance is caused by circumstances outside of Vendor's control or if a Service is properly terminated in accordance with Vendor's rights under the Agreement. In addition, support provided under this Agreement will not be withheld due to any unrelated dispute arising under this Agreement, another agreement between the Parties, or any other unrelated dispute between the Parties.

5. **Public Cloud.** Vendor will not create a public cloud account on behalf of University without prior written approval by University's IT Security team.
6. **Cloud Management.** Vendor is responsible for continuous vulnerability management of hardware and software, including, without limitation, scanning and issue remediation. Vendor is responsible for all disruptions and damage caused to any University Data while it is hosted in Cloud Software.
7. **Hosting Facilities.** University may select or restrict where University Data will be stored and where University Data can be Processed, and the Vendor will store and/or Process it there in accordance with the service terms. If a data location selection is not covered by the service terms (or a data location selection is not made by University with respect to any University Data), the Vendor will default to a United States-based data location in the selection of University storage or processing facilities. Unless stated otherwise in this Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Agreement. This provision applies to work performed by subcontractors at all tiers and to all University Data.

6.6. PCI Appendix

In addition to the terms in the AGREEMENT, the following terms will apply if the Services provided under this Agreement involve processing credit and/or debit card transactions.

1. **Payment Card Industry Data Security Standard.** For e-commerce business and/or payment card transactions, Vendor will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI Security Standards), and be solely responsible for security and maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.
2. Vendor will, at all times during the term of this Agreement, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Vendor will provide attestation of compliance to University annually by delivering to University current copies of the following: (i) Vendor's "Attestation of Compliance for Onsite Assessments – Service Providers;" (ii) an attestation that all University locations are being processed and secured in the same manner as those in Vendor's "PCI Report on Compliance;" and (iii) a copy of Vendor's PCI Report on Compliance cover letter. Vendor will notify University immediately if Vendor becomes non-compliant, and of the occurrence of any security incidents (including information disclosure incidents, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities) in accordance with the AGREEMENT.
3. Vendor's services must include the following:
 - (a) Vendor maintains its own network operating on its own dedicated infrastructure. Vendor's network includes a firewall that: (i) includes access control rules that separate Vendor's PCI network from University, and (ii) restricts any communication between Vendor's network devices and University Systems.
 - (b) Vendor treats the University Network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on University Network, and University has no ability to decrypt cardholder data.
 - (c) All devices must be SRED (secure reading and exchange of data), EMV (Europay, MasterCard and VISA) and PTS POI compliant.

6.7. PHI APPENDIX - BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“**BAA**”) is by and between the Arizona Board of Regents, acting on behalf of the University of Arizona (the “**Covered Entity**”), and **Vendor** (the “**Business Associate**”) and is part of the Underlying Agreement between the Parties. Covered Entity and Business Associate are sometimes referred to herein individually as a “Party” and collectively as the “Parties.”

Covered Entity and Business Associate have entered into an underlying agreement (“**Underlying Agreement**”), pursuant to which Business Associate performs functions or activities on behalf of, or provides certain services (collectively “**Services**”) as an independent contractor to Covered Entity, and in connection with the Services, Business Associate may have access to, or create, receive, maintain, use, or disclose Protected Health Information (“**PHI**”). The Services to be provided by Business Associate are identified in the Underlying Agreement.

Both Parties are required to comply with the Health Information Technology Economic and Clinical Health (“**HITECH**”) Act, the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) and applicable regulations issued thereunder, including, but not limited to, the Privacy, Security, Breach Notification and Enforcement Rules (45 C.F.R. Parts 160, 162 and 164), as may be amended from time to time (collectively, the “**HIPAA Rules**”). This BAA sets forth the terms and conditions pursuant to which any Protected Health Information, including electronic Protected Health Information, will be handled by Business Associate and certain third parties during the term of the Underlying Agreement and after its termination. The Parties agree as follows:

1. DEFINITIONS

All capitalized terms used but not otherwise defined in this BAA will have the meaning set forth in HIPAA/HITECH and the HIPAA Rules as in effect or as amended or supplemented from time to time. Without limiting the generality of the foregoing, the following terms, to the extent used in this Agreement, will have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Use and Workforce.

2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY BUSINESS ASSOCIATE

- (a) Performance of Services. Pursuant to the Underlying Agreement, Business Associate provides Services for Covered Entity that may involve the use and disclosure of Protected Health Information. Except as otherwise specified herein, Business Associate may use Protected Health Information to the extent necessary to perform its obligations under the Agreement, provided that (i) such use complies with and does not violate HITECH, HIPAA or the HIPAA Rules or (ii) such use is expressly permitted by this BAA. In conducting activities under the Underlying Agreement that involve the use or disclosure of Protected Health Information, Business Associate will limit the use or disclosure of Protected Health Information to the minimum amount of information necessary to accomplish the intended purpose of the use or disclosure. To the extent Business Associate is to carry out one or more of Covered Entities’ obligations under HIPAA or HITECH, Business Associate agrees to comply with the legal requirements that apply to Covered Entities in the performance of such obligation(s).
- (b) Proper Management and Administration. Except as otherwise expressly limited in this BAA or the Underlying Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that any disclosure of information received in such capacity will be made only if: (i) Required by law; or (ii) Business Associate obtains written reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any breaches of the confidentiality of the PHI.
- (c) Data Aggregation. In addition to using the Protected Health Information to perform the Services set forth in Section 2(a) of this BAA, Business Associate may use Protected Health Information for Data Aggregation purposes for the Health Care Operations of Covered Entity only, and only if expressly authorized under the Underlying Agreement. Business Associate may not de-identify Protected Health Information received from or created on behalf of Covered Entity unless such de-identification is expressly permitted by the Underlying Agreement or this BAA or unless Business Associate obtains Covered Entity’s prior written consent to such de-identification.
- (d) Prohibition on Sale of Protected Health Information. Business Associate agrees to comply with the prohibition of sale of PHI without authorization unless an exception under 45 C.F.R. §164.508 applies. This prohibition does not apply to the disclosure of PHI in connection with the Services performed under this Agreement where the only remuneration provided is for the performance of such Services, or to any other activity excluded from the definition of “Sale” under 45 C.F.R. § 164.502(a)(5)(ii).

- (e) Marketing and Fundraising. Business Associate will not use or disclose PHI for marketing or fundraising purposes, except with the prior written authorization of the Covered Entity and consistent with the requirements of 45 C.F.R. §§ 164.514(f) and 164.508(a)(3).

3. OBLIGATIONS AND RESPONSIBILITIES OF BUSINESS ASSOCIATE WITH RESPECT TO PROTECTED HEALTH INFORMATION

Business Associate hereby agrees to do the following:

- (a) Use and Disclosure of PHI. Use or disclose the Protected Health Information only as permitted or required by the Underlying Agreement or this BAA or as otherwise Required by Law. Business Associate will not, without the prior written consent of Covered Entity, disclose any Protected Health Information on the basis that such disclosure is Required by Law without first notifying Covered Entity so that Covered Entity will have an opportunity to object to the disclosure and to seek appropriate relief unless immediate disclosure is Required by Law. Business Associate will require reasonable assurances from third parties receiving Protected Health Information in accordance with Section 2(b) hereof that such third parties will provide Covered Entity with similar notice and opportunity to object before disclosing Protected Health Information on the basis that such disclosure is Required by Law. Business Associate may disclose Protected Health Information for the purposes authorized by this Agreement only (i) to members of its Workforce, (ii) to its Subcontractors (as defined below) and agents in accordance with Section 3(d), (iii) as directed by Covered Entity in accordance with this BAA, or (iv) as otherwise permitted by the terms of this BAA including, but not limited to, Section 2(b) above. Any other use or disclosure not permitted or required by this Agreement is prohibited.
- (b) Reports in Writing. Business Associate must report to the designated Privacy Officer of Covered Entity, in writing, any Breach or Security Incident of which Business Associate becomes aware as soon as possible, and at least within three (3) days of Business Associate's discovery of any of the foregoing (for purposes hereof, "discovery" will have the meaning ascribed to it in 45 CFR § 164.404(a)(2)). In the event of a Breach or Security Incident that arises from the actions or omissions of Business Associate or its employees, Subcontractors, agents, representatives or other members of its Workforce, and that requires notification of government agencies or patients, Business Associate will cooperate fully with Covered Entity in Covered Entity's efforts to carry out the notification and mitigation requirements and will indemnify and reimburse Covered Entity for all of Covered Entity's costs of complying with and carrying out such requirements.
- (c) Mitigation. Mitigate, to the greatest extent practicable, any harmful effects from any Breach or any Security Incident of which Business Associate becomes aware.
- (d) Safeguards. Comply with the Security Rule to maintain the security of, and prevent any unauthorized use or disclosure of, electronic Protected Health Information. Business Associate will maintain and implement a comprehensive information privacy and security program that complies with HITECH, HIPAA, and the regulations and guidance issued thereunder by the United States Department of Health and Human Services ("**HHS**"). Without limitation, this includes administrative, technical and physical safeguards that are appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities involving Protected Health Information. Business Associate will comply with the HHS guidance to render unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals, with respect to ePHI in motion and at rest, and destruction of PHI. In addition, in the event that the Underlying Agreement contains specific requirements regarding information and data security, Business Associate will comply with all such provisions of the Agreement.
- (e) Subcontractors. Require any person(s) to whom Business Associate delegates a function, activity or service under the Agreement (other than members of Business Associate's Workforce) or who create, receive, maintain or transmit Protected Health Information on behalf of or for Business Associate ("**Subcontractors**") and agents that receive or use, or have access to, Protected Health Information to enter into a written agreement that, (i) complies with HITECH and HIPAA, (ii) includes the same restrictions, conditions, obligations and requirements concerning Protected Health Information that apply to Business Associate pursuant to this BAA; and (iii) provides that all assignees or subcontractors of Business Associate's Subcontractor will enter into written agreements satisfying the requirements of clauses (i) through (iii) above. Before allowing any subcontractor or agent that is not organized under the laws of any state within the United States ("**Foreign Subcontractor**") to use or disclose, or have access to, Protected Health Information, Business Associate will obtain the prior written consent of Covered Entity to the use of such Foreign Subcontractor, which consent may be withheld in Covered Entity's sole discretion.
- (f) Accounting of Disclosures of PHI. Business Associate must:

Maintain and make available the information required to enable Covered Entity to respond to an individual's request for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528; and

Within five (5) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's Protected Health Information in accordance with 45 C.F.R. § 164.528.

In the event that an individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request; Covered Entity will be responsible for preparing and delivering to the individual any such accounting requested.

(g) Availability of Records for Review by HHS and Covered Entity.

Make available all records, books, agreements, policies and procedures relating to the use or disclosure of Protected Health Information to the Secretary of the U.S. Department of Health and Human Services (or any officer or employee of HHS to whom the Secretary of HHS has delegated such authority) for purposes of determining Covered Entity's compliance with the Privacy Rule and Security Rule, subject to attorney-client and other applicable legal privileges. Business Associate will immediately notify Covered Entity upon receipt by Business Associate of any complaint or request for access by the Secretary of HHS and will provide Covered Entity with a copy thereof as well as a copy of all materials disclosed pursuant thereto.

Upon reasonable prior written notice, make available during normal business hours at Business Associate's offices all policies, procedures and related materials pertaining to the use or disclosure of, and security of, Protected Health Information to Covered Entity for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of this Agreement.

4. RESPONSIBILITIES OF BUSINESS ASSOCIATE WITH RESPECT TO HANDLING OF DESIGNATED RECORD SET

In the event that the Protected Health Information received by Business Associate pursuant to the Underlying Agreement constitutes a Designated Record Set, Business Associate hereby agrees to do the following:

- (a) Access. At the request of Covered Entity, provide access to the Protected Health Information to Covered Entity for inspection or copying, to enable Covered Entity to fulfill its obligations under 45 C.F.R. § 164.524. In the event that an individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request; Covered Entity will be responsible for delivering to the individual the information he or she has requested.
- (b) Amendment. At the request of Covered Entity, make any amendment(s) to the Protected Health Information that Covered Entity directs pursuant to 45 C.F.R. § 164.526. In the event that any individual requests an amendment of Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of such request; Covered Entity will then direct Business Associate to amend its Protected Health Information, as may be appropriate based on the individual's request.

5. REPRESENTATIONS AND WARRANTIES OF BUSINESS ASSOCIATE

Business Associate represents and warrants to Covered Entity that all of its employees, agents, representatives, Subcontractors and members of its Workforce, whose services may be used to fulfill obligations under the Underlying Agreement or this BAA are or will be appropriately informed of their obligations and responsibilities regarding Protected Health Information hereunder.

6. OBLIGATIONS OF COVERED ENTITY

- (a) Changes in Permission. Covered Entity will provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI provided to it by the Covered Entity, if such changes affect Business Associate's permitted or required uses and disclosures.
- (b) Notification of Restrictions. Covered Entity will notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity or Business Associate has agreed to in accordance with 45 C.F.R. § 164.522.
- (c) Requests to Use or Disclose PHI. Covered Entity will not request that Business Associate use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by the Business Associate or the Covered Entity.

7. TERM AND TERMINATION

- (a) Term. This Agreement will become effective on the Underlying Agreement Effective Date and will continue in effect until termination or expiration of the Services Agreement, subject to the survival provisions of Section 9(a), unless terminated as provided in this Section 7.

- (b) Termination by Covered Entity. As provided under 45 C.F.R. § 164.504(e)(2)(iii), Covered Entity may immediately terminate this Agreement and the Services Agreement if Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under the provisions of this Agreement. Alternatively, if Covered Entity has determined that Business Associate has violated a material term of this Agreement and Covered Entity elects not to immediately terminate the Services Agreement and this Agreement, then Covered Entity will: (i) provide Business Associate written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure the alleged material breach within five (5) days. In the event that Business Associate does not cure the breach within five (5) days, Covered Entity may terminate, the Services Agreement or this Agreement, if feasible (as determined by Covered Entity), or if termination is not feasible, report the problem to the Secretary of HHS.
- (c) Effect of Termination. Upon termination of the Services Agreement and this Agreement pursuant to this Section 7, Business Associate must return to Covered Entity, or if agreed to by Covered Entity, destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate and its agents and Subcontractors still maintain in any form. If such return or destruction is not feasible, then Business Associate will so notify Covered Entity in writing, and will (a) extend any and all protections, obligations, limitations and restrictions contained in this BAA to Protected Health Information retained by Business Associate, its agents and its Subcontractors after the termination of the Services Agreement and this Agreement, (b) limit any further uses or disclosures to those purposes that make the return or destruction of the Protected Health Information infeasible and (c) at such time as return or destruction of such retained Protected Health Information becomes feasible, return or, if agreed to by Covered Entity, destroy such Protected Health Information.

8. INDEMNIFICATION

Business Associate agrees to indemnify and hold harmless Covered Entity and its officers, agents and employees (collectively, Covered Entity's "Indemnitees") against all actual and direct losses, liabilities, damages, claims, costs or expenses (including Covered Entity's reasonable attorney's fees in defending itself against third party claims) they may suffer as the result of third party claims, demands, actions, investigations, settlements or judgments against them arising from or in connection with any breach of this Agreement or of any representation or warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the Privacy Rule and Security Rule, by Business Associate or its employees, directors, officers, Subcontractors, agents or other members of its Workforce. Business Associate's obligation to indemnify Covered Entity and its Indemnitees will survive the expiration or termination of this BAA for any reason.

9. MISCELLANEOUS

- (a) Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 3 and 7 - 9, solely with respect to Protected Health Information Business Associate retains in accordance with Section 7(c) because it is not feasible to return or destroy such Protected Health Information, will survive termination of this Agreement indefinitely. In addition, Section 4 will survive termination of this Agreement, provided that Covered Entity determines that the Protected Health Information being retained pursuant to Section 7(c) herein constitutes a Designated Record Set.
- (b) Limitation of Liability. To the extent that the Agreement contains a provision that limits Business Associate's liability under the Underlying Agreement, Business Associate's obligations under this BAA, including but not limited to Business Associate's indemnification obligations under Sections 3(b) and 8 hereof, will be excluded from such limitation of liability.
- (c) Entire Agreement; Amendments; Waiver. This BAA constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes any previous agreements between the Parties relating to the same subject matter. This BAA may not be modified, nor will any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event cannot be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.
- (d) No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.
- (e) Notices. Any notices to be given under this BAA to a Party will be made via U.S. Mail or express courier to such Party's address set forth below, or via facsimile to the facsimile telephone numbers listed below.

Covered Entity Contact:

As stated in the Underlying Agreement.

With a copy to:

HIPAA Privacy Officer
The University of Arizona
PO Box 210409
Tucson, AZ 85721
Fax: (520) 621-3355

Business Associate Contact:

As stated in the Underlying Agreement.

Each Party may change its address and that of its representative for notice by giving notice thereof in the manner provided above in this Section 9(e).

- (f) Applicability. If the provision of Services involves Business Associate's receipt, maintenance or transmission of University Data that contains PHI, the Parties agree that this BAA shall become an integral part of the Underlying Agreement and shall apply to Business Associate's receipt, maintenance or transmission of PHI from, or on behalf of the Covered Entity.
- (g) Interpretation; Inconsistences between Agreement and BAA; Section Headings. The provisions of this BAA will prevail over any provisions in the Underlying Agreement that may conflict or appear inconsistent with any provisions in this BAA. The Parties agree that any ambiguity in this BAA will be resolved in favor of a meaning that complies and is consistent with the Privacy Regulation and Security Regulation. The section headings used in this BAA are for reference and convenience only and have no legal or contractual effect.
- (h) Governing Law. This BAA will be governed by and construed in accordance with the laws of the State of Arizona, without application of principles of conflicts of laws. The Parties hereto agree that any dispute arising under this contract will be resolved in the Arizona State courts of Pima County, Arizona or in the Federal District Court for the District of Arizona sitting in Tucson, Arizona, and the Parties hereby submit themselves to the personal jurisdiction of said courts.
- (i) Amendment to Comply with Law. The Parties agree to take such action as is necessary to implement the standards and requirements of HITECH and regulations thereunder, HIPAA, the Privacy Regulation, the Security Regulation, and other applicable laws relating to the security or confidentiality of Protected Health Information. The Parties further agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of HITECH, HIPAA, the HIPAA Rules or other applicable laws.
- (j) State Law. Nothing in this BAA will be construed to require or permit Business Associate to use or disclose Protected Health Information without written authorization from an individual who is a subject of the Protected Health Information, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.
- (k) Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this BAA will cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law, in equity, or under this BAA, in the event of any violation of any of the provisions of this BAA, or any explicit threat thereof, Covered Entity will be entitled to an injunction or other decree of specific performance with respect to such violation(s) or explicit threat thereof.
- (l) Agency. The Parties agree and acknowledge that Business Associate is not an "agent" of Covered Entity as that term is defined in the federal common law.

The rest of this page left blank intentionally.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf as of the Effective Date

COVERED ENTITY: The University of Arizona

BUSINESS ASSOCIATE

Signature of Authorized Representative

Signature of Authorized Representative

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Reviewed by: THE UNIVERSITY OF ARIZONA HIPAA PRIVACY OFFICER

Signature of Acknowledgement

Printed Name: **John F Howard**

Date: _____