March 12, 2018

REQUEST FOR PROPOSAL

FREELANCER PLATFORM

RFP 301802

DUE: 3:00 P.M., MST, 4/3/18

Time and Date of Pre-Proposal Conference	3:00 P.M., MST, 3/19/18
Deadline for Inquiries	3:00 P.M., MST, 3/21/18
Time and Date Set for Closing	3:00 P.M., MST, 4/3/18

TABLE OF CONTENTS

SECTION I – REQUEST FOR PROPOSAL

RFP 301802

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Freelancer Platform Proposal.**

Proposals are to be addressed and delivered to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, (located on the east side of Rural Road between Apache Road & Broadway Road) Tempe, Arizona 85281 **on or before 3 PM on April 3rd, 2018** at which time a representative of Purchasing and Business Services will announce publicly the names of those firms or individuals submitting proposals**. No proposals will be accepted after this time.** No other public disclosure will be made until after award of the contract.

Arizona State University's Overnight Delivery (FedEx, Airborne, and UPS) address is:

Purchasing and Business Services
University Services Building
Arizona State University
1551 S. Rural Rd
Tempe, AZ 85281

Arizona State University's U.S. Postal Service Mail address is:

Purchasing and Business Services
Arizona State University
P.O. Box 875212
Tempe, AZ 85287-5212

ARIZONA STATE UNIVERSITY

Allyson Taylor

_____
Allyson Taylor
Buyer

AT/AP

SECTION II – PURPOSE OF THE RFP

1. INTENT

The increasing demand for technical talent within the University Technology Office (UTO) is the primary reason for initiating this RFP. Additionally, within ASU there are a number of other departments and verticals that have a need to rapidly secure IT talent and still other areas of the University similarly need to secure talent that is not specific to IT. For example, Departments such as Marketing, HR, Purchasing and Legal may also benefit from using the Freelancer Platform. The purpose of this RFP is to select a Freelancer Platform(s) that will be an enterprise solution for ASU. Because it may not be possible for a single platform to provide such a comprehensive freelancer base, it is possible that the outcome of this RFP will be the selection of multiple Freelancer Platforms that will cumulatively provide the needed enterprise solution. To qualify for consideration, all Freelancer Platform proposals are expected to meet the evaluation criteria stated herein.

Key objectives of implementing a Freelancer Platform include:

- Access to the growing, highly skilled freelancer talent pool.
- Ability to more rapidly identify and hire temporary staff.
- Increased visibility and control of the work of temporary staff.
- Reduced temporary staffing expenses.

2. BACKGROUND INFORMATION

The University Technology Office has a technology rich environment with projects that span numerous applications and platforms. The associated technology stack presents opportunities for freelancers from many disciplines.

This list identifies examples of key positions and disciplines that the University Technology Office (UTO) may require the freelance platform to supply. However the intent of using freelance options at the ASU enterprise level will likely lead to other resource options than those used by the University Technology Office.

(In Alphabetical order)

- Application Software Engineers
- Business Analysts
- Business Intelligence Analysts
- Cloud Network Engineering
- Data Analysts
- Data Architects
- Database Administrators
- Database Designers
- Instructional Designers
- Instructional Technical Analysts
- Java Software Engineers
- Network Engineers
- Peoplesoft Developers
- Project Managers
- Quality Assurance Analysts

- Salesforce Administrators
- Salesforce Developers
- Security Administrators
- Security Analysts
- Security Architects
- Security Engineers
- Server Administrators
- Software Application Analysts
- Software Application Developers
- Systems Administrators
- Systems Analysts
- Systems Architects
- Systems Support Analysts (Desktop Support)
- Systems Support Engineers
- Technical Support Analysts
- Technical Writers
- Web Application Designers
- Web Dashboard Developers
- Web Developers
- Web User Experience Designers (UX)

For additional background on UTO's projects and initiatives, please visit www.asu.edu/UTO

Arizona State University is a new model for American higher education, an unprecedented combination of academic excellence, entrepreneurial energy and broad access. This New American University is a single, unified institution comprising four differentiated campuses positively impacting the economic, social, cultural and environmental health of the communities it serves. Its research is inspired by real world application blurring the boundaries that traditionally separate academic disciplines. ASU serves more than 91,000 students in metropolitan Phoenix, Arizona, the nation's fifth largest city. ASU champions intellectual and cultural diversity, and welcomes students from all fifty states and more than one hundred nations across the globe.

If you would like more information about ASU, please visit us via the World Wide Web. Our home page address is http://www.asu.edu.

3. TERM OF CONTRACT

The initial contract term will be for one (1) year(s) with the possibility of four (4) successive one (1) year renewals, for a total term not to exceed five (5) years. The contract will be available for use by other University departments during this term.

SECTION III – PRE-PROPOSAL CONFERENCE

A pre-proposal conference will be held at 3 PM MST on March 19th, 2018 via Adobe Connect.

The purpose of this conference will be to clarify the contents of this Request for Proposal in order to prevent any misunderstanding of the University's intention and desires, and/or to give prospective suppliers an opportunity to review the site of the work. Any doubt as to the requirements of this solicitation, or any apparent omission or discrepancy should be presented to the University representative at this conference. The University representative will then determine the appropriate action. If necessary, the University representative will issue a written amendment to this Request for Proposal. Oral statements or instructions shall not constitute an amendment to this Request for Proposal.

You do not have to send a representative to this pre-proposal conference. However, if you decide to not send a representative, then we may not know of your intent to participate in this Request for Proposal, and so may not send you any written amendments to this Request for Proposal. Further, we will assume that your failure to attend the pre-proposal conference is an indication that you expect us to review your proposal as if you had taken advantage of the pre-proposal conference.

To participate in the pre-proposal conference, complete the following:

1. Register by 5 PM MST Friday, March 16th, 2018 for the event by sending an email of participants to include to allyson.taylor@asu.edu. Include the following information:
    a. First and last name
    b. Company
    c. Title
    d. Email address
    e. Phone number

2. On the day of the conference, registered users will be provided a passcode to enter the virtual room.

    On the day of the conference, go to connect.asu.edu.

    Only registered users may enter the room, guest access is blocked.

3. Once entered, the conference audio information will be provided.

SECTION IV – INSTRUCTIONS TO PROPOSERS

1. You must address and deliver your proposal to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, Tempe, Arizona 85281, **on or before the time and date set for closing. No proposal will be accepted after this time.** The University Services Building is located on the east side of Rural Road between Apache Road and Broadway Road. **PROPOSALS MUST BE IN A MARKED SEALED CONTAINER** (i.e., envelope, box):

Name of Proposer
Title of Proposal
RFP Number
Date and Time Proposal is Due

No telephone, electronic or facsimile proposals will be considered. **Proposals received after the time and date for closing will be returned to the proposer unopened.**

2. **DIRECTIONS TO USB VISITOR PARKING**. Purchasing and Business Services is in the University Services Building ("USB") 1551 S. Rural Road, Tempe, AZ, 85281 (located on the east side of Rural between Broadway Ave and Apache Boulevard). A parking meter is located near the main entry to USB.

All visitors to USB are required to check in at the USB Reception Desk to obtain a visitor's badge to wear while in the building. The receptionist will call to have you escorted to your meeting.

3. Proposer should use recycled paper and double-sided copying for the production of all printed and photocopied proposal documents. Furthermore, the documents should be clearly marked to indicate that they are printed on recycled content (minimum 30% post-consumer waste paper).

4. You may withdraw your proposal at any time prior to the time and date set for closing.

5. No department, school, or office at the University has the authority to solicit or receive official proposals other than Purchasing and Business Services. All solicitations are performed under the direct supervision of the Chief Procurement Officer and in complete accordance with University policies and procedures.

6. The University reserves the right to conduct discussions with proposers, and to accept revisions of proposals, and to negotiate price changes. During this discussion period, the University will not disclose any information derived from proposals submitted, or from discussions with other proposers. Once a contract is executed, the solicitation file, and the proposals contained therein, are in the public record and will be disclosed upon request.

7. Proposers submitting proposals which meet the selection criteria and which are deemed to be the most advantageous to the University may be requested to give an oral presentation to a selection committee. Purchasing and Business Services will do the scheduling of these oral presentations.

8. The award shall be made to the responsible proposer whose proposal is determined to be the most advantageous to the University based on the evaluation factors set forth in this solicitation. Price, although a consideration, will not be the sole determining factor.

9. If you are submitting any information you consider to be proprietary, you must place it in a separate envelope and mark it "Proprietary Information". If the Chief Procurement Officer concurs, this information will not be considered public information. The Chief Procurement Officer is the final authority as to the extent of material, which is considered proprietary or confidential. Pricing information cannot be considered proprietary.

10. The University is committed to the development of Small Business and Small Disadvantaged Business ("SB & SDB") suppliers. If subcontracting (Tier 2 and higher) is necessary, proposer (Tier 1) will make every effort to use SB & SDB in the performance of any contract resulting from this proposal. A report may be required at each annual anniversary date and at the completion of the contract indicating the extent of SB & SDB participation. **A description of the proposers expected efforts to solicit SB & SDB participation should be enclosed with your proposal.**

11. Your proposal should be submitted in the format shown in Section X. Proposals in any other format will be considered informal and may be rejected. Conditional proposals will not be considered. An individual authorized to extend a formal proposal must sign all proposals. Proposals that are not signed may be rejected.

12. The University reserves the right to reject any or all proposals or any part thereof, or to accept any proposal, or any part thereof, or to withhold the award and to waive or decline to waive irregularities in any proposal when it determines that it is in its best interest to do so. The University also reserves the right to hold all proposals for a period of **one hundred and twenty (120) days** after the opening date and the right to accept a proposal not withdrawn before the scheduled proposal opening date.

13. **EXCEPTIONS:** Proposer is expected to enter into a standard form of agreement approved by the Arizona Board of Regents. The Arizona State University contract terms and conditions are included in this Request for Proposal in Section XII. These terms and conditions are intended to be incorporated into the contract between the University and the successful proposer. **Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed non responsive and may be rejected.**

14. Unless specifically stated to the contrary, any manufacturer's names, trade names, brand names or catalog numbers used in the specifications of this Request for Proposal are for the purpose of describing and/or establishing the quality, design and performance required. Any such reference is not intended to limit or restrict an offer by any proposer and is included in order to advise the potential proposer of the requirements for the University. Any offer, which proposes like quality, design or performance, will be considered.

15.

Days:	Calendar days
May:	Indicates something that is not mandatory but permissible/desirable.
Shall, Must, Will:	Indicates mandatory requirement. Failure to meet these mandatory requirements will result in rejection of your proposal as non-responsive.
Should:	Indicates something that is recommended but not mandatory. If the proposer fails to provide recommended information, the University may, at its sole option, ask the proposer to provide the information or evaluate the proposal without the information.

16. Any person, firm, corporation or association submitting a proposal shall be deemed to have read and understood all the terms, conditions and requirements in the specifications/scope of work.

17. All proposals and accompanying documentation will become the property of the University at the time the proposals are opened. **It will be the proposer's responsibility to request that samples be returned to the proposer and provide a method for doing so at the expense of the proposer.** If a request is not received and a method of return is not provided, all samples shall become the property of the University 45 days from the date of the award.

18. All required performance and payment bonds shall be held by the University in a secure location until the performance of the contract and the payment of all obligations rising there under have been 100% fulfilled. Upon completion of the project and all obligations being fulfilled, it shall be the proposer's responsibility to request the surety bonding company to submit to the University the necessary documents to approve the release of the bonds. Until such time the bonds shall remain in full force and effect.

19. The University of Arizona, Northern Arizona University, and Arizona State University are all state universities governed by the Arizona Board of Regents. **Unless reasonable objection is made in writing as part of your proposal to this Request for Proposal, the Board or either of the other two Universities may purchase goods and/or services from any contract resulting from this Request for Proposal.**

20. The University has entered into Cooperative Purchasing Agreements with the Maricopa County Community College District and with Maricopa County, in accordance with A.R.S. Sections 11-952 and 41-2632. Under these Cooperative Purchasing Agreements, and with the concurrence of the proposer, the Community College District and/or Maricopa County may access a contract resulting from a solicitation done by the University. If you do not want to grant such access to the Maricopa County Community College District and or Maricopa County, **please state so** in your proposal. In the absence of a statement to the contrary, the University will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

21. Arizona State University is also a member of the Strategic Alliance for Volume Expenditures ($AVE) cooperative purchasing group. $AVE includes the State of Arizona, many Phoenix metropolitan area municipalities, and many K-12 unified school districts. Under the $AVE Cooperative Purchasing Agreement, and with the concurrence of the proposer, a member of $AVE may access a contract resulting from a solicitation done by the University. If you **do not** want to grant such access to a member of $AVE, **please state so** in your proposal. In the absence of a statement to the contrary, the University will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

22. All formal inquiries or requests for significant or material clarification or interpretation, or notification to the University of errors or omissions relating to this Request for Proposal must be directed, in writing or by facsimile, to:

Allyson Taylor
Purchasing and Business Services
University Services Building
Arizona State University
PO Box 875212

Tempe, AZ 85287-5212

Tel: 480-965-2074
E-mail: allyson.taylor@asu.edu

Requests must be submitted on a copy of the Proposer Inquiry Form included in Section XI of this Request for Proposal. All formal inquiries must be submitted at least ten (10) calendar days before the time and date set for closing this Request for Proposal. Failure to submit inquiries by this deadline may result in the inquiry not being answered.

Note that the University will answer informal questions orally. The University makes no warranty of any kind as to the correctness of any oral answers and uses this process solely to provide minor clarifications rapidly. Oral statements or instructions shall not constitute an amendment to this Request for Proposal. Proposers shall not rely on any verbal responses from the University.

23. The University shall not reimburse any proposer the cost of responding to a Request for Proposal.

24. In accordance with an executive order titled "Air Pollution Emergency Proclamation" modified by the Governor of Arizona on July 16, 1996, the University formally requests that all products used in the performance of any contract that results from this Request for Proposal be of low- or no-content of reactive organic compounds, to the maximum extent possible.

25. Arizona requires that the University purchase ENERGY STAR® products or those certified by the Federal Energy Management Program as energy efficient in all categories available. If this Request for Proposal is for a product in a category for which ENERGY STAR® or certified products are available, please submit evidence of the ENERGY STAR® status or certification for the products you are bidding. Please note that if you fail to submit this information but a competitor does, the University will select your competitor's product as meeting specifications and deem your product as not meeting specifications. See A.R.S. §34-451.

26. The University requires that all desktop computers, notebooks, and monitors purchased must meet Electronic Product Environmental Assessment Tool (EPEAT) Gold status as contained in the IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products. The registration criteria and a list of all registered equipment are at http://www.epeat.net/about-epeat/ on the Web.

27. To the extent applicable to any contract resulting from this Request for Proposal, the proposer shall comply with the Standards for Privacy of Individually Identifiable Information under the Health Insurance Portability and Accountability Act of 1996 contained in 45 CFR Parts 160 and 164 (the "HIPAA Privacy Standards") as of the effective date of the HIPAA Privacy Standards on April 14, 2003 or as later determined. Proposer will use all security and privacy safeguards necessary to protect Protected Health Information (PHI), as defined by HIPAA, and shall immediately report to University all improper use or disclosure of PHI of which it becomes aware. Proposer agrees to ensure that its agents and subcontractors agree to and abide by these requirements. **Proposer agrees to indemnify the State of Arizona, its departments, agencies, boards, commissions, universities and its officers, officials, agents, and employees against all harm or damage caused or contributed to by proposer's breach of its obligations under this paragraph.**

28. The University believes that it can best maintain its reputation for treating suppliers in a fair, honest, and consistent manner by conducting solicitations in good faith and by granting competitors an equal opportunity to win an award. If you feel that we have fallen short of these goals, you may submit a protest pursuant to the Arizona Board of Regents procurement procedures, section 3-809, in particular section 3-809C. This paragraph does not include all of the provisions of the Regents procedures, but it does tell you what you have to do to initiate a protest. First, you have to be an "interested party." An "interested party" is an actual or prospective proposer whose direct economic interest may be affected by the issuance of a solicitation, the award of a contract, or by the failure to award a contract. Whether an actual prospective bidder or offeror has a *direct* economic interest will depend upon the circumstances in each case. At a minimum, the interest must be substantial and must be tangibly affected by the administrative action or proposed action concerned in the case. For instance, a bidder or proposer who is fourth in line for award does not have a sufficient economic interest to protest the proposed award of a contract to the low bidder or offeror. Second, you must submit the protest in a timely manner. In procurements inviting bids, protests based upon alleged errors, irregularities or, improprieties in a solicitation that are apparent before the bid opening shall be filed before the bid opening. In procurements requesting proposals, protests based upon alleged errors, irregularities or improprieties in a solicitation that are apparent before the closing date for receipt of initial proposals shall be filed before the closing date for receipt of initial proposals. Protests concerning improprieties that do not exist in the initial solicitation, but that are subsequently incorporated into the solicitation, shall be filed by the next closing date for receipt of proposals following the incorporation. In cases other than those just covered, protests shall be filed no later than ten (10) days after a contract is awarded in connection with the procurement action. Failure to timely protest shall be deemed a waiver of all rights. Third, and finally, your protest shall be in writing and shall include the following information: (1) The name, address, telephone number, and fax number of the protester; (2) The signature of the protester or its representative; (3) Identification of the solicitation or contract number; (4) A detailed statement of the legal and factual grounds of the protest including copies of relevant documents; and (5) The form of relief requested.

Protests should be directed to:

Jamon Hill
Deputy Chief Procurement Officer
Purchasing and Business Services
PO Box 875212
Tempe AZ 85287-5212
Email: Jamon.Hill@asu.edu

Please note that as the University takes protests very seriously; we expect you to do so as well. Frivolous protests will not result in gain for your firm.

SECTION V – SPECIFICATIONS/SCOPE OF WORK

Integration of a talent platform into a public organization as broad and diverse as ASU has a number of technical, legal, security, financial and other compliance requirements that must be considered.

There are both questions and statements regarding the requirements set forth. **Please specify directly under each subheading how the freelancer platform that your organization is proposing meets these requirements.**

Organizational / Platform Data:

- Provide a description of the basic functionality and operational elements of your platform.
- Describe how ASU administrative users would logon and access the platform.
- How do you suggest our organization access your platform? With administrative accounts? Named users? How many users do you suggest for an organization of our size?
- Describe how ASU would post a position / project to be seen by freelancers.

Access to Qualified Freelancers:

- Does the freelancer platform have access to a US-based, technically diverse freelancer candidate pool with a proven project completion record?
- Does the freelancer platform have access to an international, technically diverse freelancer candidate pool with a proven project completion record?
- Describe the process it would take for a freelancer to join your platform. Please include the amount of time it would take to do so and what elements would be asked of the freelancer during this process.
- Confirm that the Freelancer Platform will allow ASU students to sign up as freelancers.
- Describe how risk is managed and minimized when working across international lines.
- How does your organization comply with GDPR requirements?
- Does the technical diversity of the pool support the position / skillset needs described in Section II of the RFP?

Online Collaboration Technology:

- Does the platform provide secure user permissions that enable teams to chat, video, and share files in real time?

US Employment Status Visibility:

- If the freelancer is not a US Citizen, Permanent Resident or Green Card holder, the freelancer's visa status must be disclosed. How would this criteria be met by your platform and communicated to us as a user?

Onboarding:

- Does the platform provide a fully-configured dashboard with onboarding that includes the following requirements in order to help freelancers start quickly in compliance with ASU policies?
    - Non-disclosure agreements
    - Security requirements

- Background checks

Enterprise Billing:

- It is preferred that that Freelancer platform have the ability to advance payments to freelancers and send ASU a single invoice with net 30 payment terms for all transactions and fees assessed on the account. Confirm that your billing process meets this criteria and if it does not, please describe your billing process.

Compliance Services:

- The platform must classify workers as either independent contractors or employees and indemnify ASU from worker misclassification risk. Provide details on how freelancers are classified.

Talent Sourcing Support:

- The Freelancer Platform must have the ability to easily profile and match position requirements with top freelancers across any skill category. Explain how specific freelancers are identified on the platform.

Program Management Support:

- The Freelancer Platform must have a service to search for freelancers and design, develop, staff and execute projects that require multiple freelancers. Explain, with details, how this is accomplished on the platform.

Protection of Intellectual Property (IP):

- The freelancer platform must demonstrate a basis for indemnifying ASU from any misuse or abuse of IP and state the actions that the freelancer platform provider will take in a case wherein a freelancer fails to adhere to ASU's IP directives.

Reporting:

- The Freelancer Platform must provide a roll-up reporting dashboard that provides a quick and real-time glance into all activity and spend associated with ASU's account. It must be able to quantify productivity and display expenses to date over project cost projections and budget. The platform must allow reporting by individual freelancer, project team or department.

Implementation:

- Provide a detailed process of how the Technical Implementation will be accomplished including a timeline.
- Provide a detailed process of how the Program Implementation will be accomplished including a timeline.
- How long does it take to get a new organization to become fully active on your platform?

Technical Implementation

- How will the following items be configured into ASU's Enterprise account?

- **Custom fields:** client-defined fields to be captured on each project or transaction such as cost centers, purchase orders, or departments.

- **Onboarding tasks**: nondisclosure agreements, independent contractor classification requirements, background checks, system security policies, data security policies, hardware policies, software policies.

- **Default contract terms:** documents that govern the lifecycle of each freelancer engagement such as Statement of Work (SOW) agreements, user provisioning and billing methods.

Program Design and Implementation

- Demonstrate how a dedicated team will work with ASU on platform adoption as well as on an ongoing basis to assist with change management including:
  - Program road-mapping
  - Program education
  - Program user training

User Roles and Permissions:

- Two key roles that need to be defined are Platform Administrator and Hiring Manager. Please describe how these roles will include the following capabilities:

1. **Administrator Permissions:**

   • Managing payment methods
   • Viewing financial reports
   • Making deposits and withdrawals
   • Inviting or removing team members
   • Managing member permissions
   • Editing company information

2. **Hiring Manager Permissions:**

   • Posting jobs and inviting freelancers to interview
   • Reviewing proposals and making contract offers
   • Ending contracts and submitting freelancer feedback
   • Giving bonuses and increasing rates

Security and Privacy

Arizona State University considers one of its paramount responsibilities to be the protection and security of University data. The purpose of the following security matrix is to assure that freelancer exposure to university data aligns with University data security standards and policies. Please describe how your platform ensures that freelancers will comply with these security requirements. It will be expected that they are agreeable to the processes outlined as they are assigned to projects by our organization.

Security & Risk Level	Data Handling Level of Access	Freelancer Requirements for Access based on Scope of Work	ASU Requirements for Access based on Scope of Work
ASU Level 0	**Limited Public or None:** Refers to having no access to any data or limited access to data that has been extracted and purged of any Level 2 of above data. Code extracts would be provided and no direct access into production environments to ensure no adverse effect on the University's operations, assets, reputation or obligations concerning information privacy or on any individual's privacy.	• Background check conducted by Freelancer Platform Provider • Non-Disclosure Agreement signed by Freelance worker • Freelance worker must abide by ACD 125: Computer, Internet, and Electronic Communications Information Management Policy	• Isolate environments to restrict access to Level 1-4 Data Categories • Access to code and data extracts • No direct access into production environments
ASU Level 1	**Public:** Public refers to information that is publicly available and intended for public use. When used as intended, this information would have no adverse effect on the University's operations, assets, reputation or obligations concerning information privacy or on any individual's privacy.	• Background check conducted by Freelancer Platform Provider • Freelance worker must abide by ACD 125: Computer, Internet, and Electronic Communications Information Management Policy • Non-Disclosure Agreement signed by Freelance worker	• Isolate environments to restrict access to Level 2-4 Data Categories • Possible access to code and data extracts • No direct access into production environments
ASU Level 2	**Internal:** Internal refers to information that is reserved for private viewing, pending public release, opt-out directory information or internal University communications.	• Background check conducted by Freelancer Platform Provider • Freelance worker must abide by ACD 125: Computer, Internet, and Electronic Communications Information Management Policy • Non-Disclosure Agreement signed by Freelance worker	• Isolate environments to restrict access to Level 3-4 Data Categories • Possible access to view code and data extracts • No direct access into any environment containing sensitive data • Code reviews conducted prior to deployment into any environment containing sensitive data and/or critical systems
ASU Level 3	**Sensitive:** Sensitive refers to information intended for limited use within the University by faculty, researchers, staff, students or University affiliates, including information that is regulated or must be protected due to proprietary or privacy concerns; e.g. private student records according to FERPA, personal health information (PHI) according to HIPAA), personally identifiable information (PII) according to state and federal laws and industry regulations. PII references: General Services Administration – Rules and Policies – Protecting PII – Privacy Act, NIST Guide to Protecting the Confidentiality of PII Unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on the University, its students or employees. Violation of statutes, regulations, or other legal obligations, actual or potential financial loss, damage to the University's reputation and possible legal action could occur.	• Background check conducted by Freelancer Platform Provider • Fingerprint registration by Freelance worker • Non-Disclosure Agreement signed by Freelance worker • FERPA & HIPAA compliance training provided by ASU and completed by Freelance worker • Freelance worker must abide by ACD 125: Computer, Internet, and Electronic Communications Information Management Policy	• Isolate environments to restrict access to Level 4 Data Categories • Possible access to view, update, and/or deploy code and data extracts • No direct access into production environments • Code reviews conducted prior to deployment into any environment containing sensitive data and/or critical systems
ASU Level 4	**Highly Sensitive:** Highly Sensitive refers to information involving human health, life, and safety matters or hazardous materials situations. This information is intended for extremely limited use within the University on a need to know basis. Statutes, regulations, other legal obligations or mandates protect much of this information. Unauthorized disclosure, compromise or destruction would result in severe damage to the University, its students or employees or other individuals providing the information. Physical harm or endangerment, violation of legal obligations, actual or potential financial loss, damage to the University's reputation and possible legal action could occur.	• Freelance worker would abide by all policies and procedures for ASU Staff & Faculty	• Possible access to code and data extracts • No direct access into production environments • If access into systems is required role-based access with granular controls will be designated

Here is the ASU Hiring requirements documentation- ACD126 Reference Checks and Background Verification - https://www.asu.edu/aad/manuals/acd/acd126.html

Waivers Compensating Controls & Approvals:

- Waivers for compensating controls can be submitted to the ASU Sponsoring Executive and Chief Information Security Office (CISO). The following process would be followed:

1) Freelancer or ASU Sponsoring Executive submits a request for waiver of specific compensating control(s).
2) CISO reviews and highlights risks.
3) ASU Sponsoring Executive either accepts risks and approves waiver or disapproves waiver.

Value-Added Services

Describe any special resources, skills, or services which the firm possess, and which are not addressed as part of this RFP, that would be available as part of an agreement with successful proposer. Please demonstrate any advantages that would be realized by the University as a result of these value-added resources.

SECTION VI – Green Purchasing Requirements/Specifications

In order to reduce the adverse environmental impact of our purchasing decisions the University is committed to buying goods and services from manufacturers and suppliers who share the University's environmental concern and commitment. Green purchasing is the method wherein environmental and social considerations are taken with equal weight to the price, availability and performance criteria that we use to make purchasing decisions.

Proposer shall use environmentally preferable products, materials and companies where economically feasible. Environmentally preferable products have a less or reduced effect on human health and the environment when compared to other products and companies that serve the same purpose. If two (2) products are equal in performance characteristics and the pricing is within 5%, the University will favor the more environmentally preferable product and company.

If you are citing environmentally preferred product claims, you must provide proper certification or detailed information on environmental benefits, durability and recyclable properties.

The University and the supplier may negotiate during the contract term to permit the substitution or addition of Environmentally Preferable Products (EPPs) when such products are readily available at a competitive cost and satisfy the university's performance needs.

Unless otherwise specified, proposers and contractors should use recycled paper and double-sided copying for the production of all printed and photocopied documents. Furthermore, the documents shall be clearly marked to indicate that they are printed on recycled content (minimum 30% post-consumer waste) paper.

Proposer shall minimize packaging and any packaging/packing materials that are provided must meet at least one of, and preferably all, of the following criteria:

Made from 100% post-consumer recycled materials
Be recyclable
Reusable
Non-toxic
Biodegradable

Further, proposer is expected to pick up packaging and either reuse it or recycle it. This is a requirement of the contract or purchase order.

SECTION VII – PROPOSER QUALIFICATIONS

The University is soliciting proposals from firms, which are in the business of providing services as listed in this Request for Proposal. Your proposal shall include, at a minimum, the following information. Failure to include these items may be grounds for rejection of your proposal.

1. The proposer shall present evidence that the firm or its officers have been engaged for at least the past three (3) years in providing services as listed in this Request for Proposal.

2. Financial Statements:

Option A. Proposers who have audited financial statements are to provide the following:

Audited financial statements for the two (2) most recent available years. If the financial statements are intended to be confidential, please submit one (1) copy in a separate sealed envelope and mark as follows:

Firm's Name
Confidential – Financial Statements

Option B. Proposers who might not have audited financial statements are to provide the following:

It is preferred that audited financial statements for the two (2) most recent available years be submitted. However, if not available, provide a copy of firm's two (2) most recent tax returns or compiled financial statements by an independent CPA. If the financial statements or tax returns are intended to be confidential, please submit one (1) copy in a separate sealed envelope and mark as follows:

Firm's Name
Confidential – Financial Statements

3. The proposer must provide the contract agreement or terms that they enter into with the freelancers and individuals that register on their platform.

4. The proposer shall provide a statistical report(s) that identifies the following criteria:

a. How many organizations overall are currently using your platform
b. How many higher educational institutions are currently using your platform
    i. How many of these institutions are public universities (if possible, please also provide the names of these universities)
c. How many organizations are using your platform at an enterprise solution level
d. How many freelancers are registered on your platform
e. How many freelancers are US-based versus international
f. The percentage of your freelancers that are US-based
g. Other metrics on your freelancer population demographics
h. How many freelancers on your platform that are specific to Information Technology
i. How long your organization has been in business

5. Submit three (3) public company or university client references comparable in scope of this RFP. References should be verifiable and should be able to comment on the firm's experience, with

a preference related to services similar to this project. Include the name, title, telephone number, and e-mail address of the individual at the client organization who is most familiar with this engagement.

6. Please provide a copy of the resume(s) of the individual(s) that will be the single point of contact between our organization and yours. Any key personnel proposed by the firm should have relevant experience, and be fully qualified to successfully provide the services described in the Scope of Work. Provide an organizational chart that provides organizational sections, with the section that will have responsibility for performing this project clearly noted.

7. The proposer will review and provide acceptance of ASU's terms and conditions. Note: all exceptions with justification and alternative language MUST be submitted with the proposal for ASU's consideration.

SECTION VIII – EVALUATION CRITERIA

Proposals will be evaluated on the following criteria, listed in order of their relative priority with most important listed first:

1. Detailed response to the Scope of Work - Section V (40%)

2. Response to the Pricing Schedule and Attachment A - Section IX (30%)

3. Detailed response to the Proposer Qualifications - Section VII (10%)

4. Acknowledgment and acceptance of the terms and conditions of the License Agreement including Insurance Requirements (Section XII). All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal. - Section XII (10%)

5. Sustainability Efforts – Section VI and Supplier Sustainability Questionnaire. (10%)

Confidential and/or proprietary information must be submitted per the instructions in Section IV, item 9. Any watermarks, footnotes, or references to confidential and/or proprietary throughout the submitted proposal will be disregarded as boilerplate markings.

SECTION IX – PRICING SCHEDULE

Proposer shall submit a detailed cost proposal to include all aspects of providing the scope of work associated with this Request for Proposal.

ATTACHMENT A-MUST BE COMPLETED AND SUBMITTED WITH YOUR PROPOSAL

The Financial proposal shall contain the complete financial offer made to the University. Any additional costs, fees, and expenses must be detailed in the proposer's proposal. Any additional expenses, not explicitly stated, will not be honored by ASU.

SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS

Format of Submittal

To facilitate direct comparisons, your proposal must be submitted in the following format:

- **One (1)** clearly marked hard copy "original" in 8.5" x 11" double-sided, non-binding form. No metal or plastic binding – may use binder, folder, or clip for easy removal of proposal. **And**

- **One (1) "single"** continuous (no folders) electronic copy (**flash drive only**), PC readable, labeled and no passwords.

  Any confidential and/or proprietary documents must be on a separate flash drive and labeled appropriately.

- Proposer must check all flash drives before submitting. Company marketing materials should not be included unless the Request for Proposal specifically requests them. All photos must be compressed to small size formats.

Content of Submittal

If proposer fails to provide any of the following information, with the exception of the mandatory proposal certifications, the University may, at its sole option, ask the proposer to provide the missing information or evaluate the proposal without the missing information.

1. Mandatory certifications, Voluntary Product Accessibility Template (VPAT), Sustainability Questionnaire, and Substitute W-9 as per Section XIII.
2. Acceptance of ASU's RFP terms and conditions: Note: all exceptions with justification and alternative language MUST be submitted with the proposal.
3. Detailed Response to Specifications/Scope of Work
4. Detailed Response to Proposer Qualifications - Section VII
5. Response to Pricing Schedule - Section IX and Attachment A

SECTION XI – PROPOSER INQUIRY FORM

Pre-Proposal Questions, General Clarifications, etc.

PROJECT NAME: Freelancer Platform

PROPOSAL NUMBER: 301802

INQUIRY DEADLINE: 3:00 P.M., MST, March 21, 2018

QUESTIONS ON: _____ ORIGINAL PROPOSAL or _____ ADDENDUM NO. _____

DATE: _____

WRITER: _____

COMPANY: _____

E-MAIL ADDRESS: _____

PHONE: _____ FAX: _____

QUESTIONS:

SECTION XII – TERMS & CONDITIONS

Arizona State University
INDEPENDENT CONTRACTOR AGREEMENT FOR CONSULTING, SERVICES, AND DELIVERABLES

THIS AGREEMENT is made between the Arizona Board of Regents, a body corporate, for and on behalf of Arizona State University (ASU) and _____, a _____ (Vendor), effective as of _____, 2018 (the Effective Date).

In consideration of the mutual obligations specified in this Agreement, the parties agree as follows:

1. Engagement; Services and Deliverables. ASU retains Vendor, as of the Effective Date, and Vendor accepts such engagement, to perform the services as and when described on Exhibit A (the Services). As part of the Services, Vendor will deliver to ASU all goods, services, reports, code, documents, software, and other materials, all of which are included in the definition of Services, as may be set forth on Exhibit A.

2. Compensation. ASU will pay Vendor for the Services as and when set forth on Exhibit A and in a Statement of Work (SOW). Unless described with specificity on Exhibit A or an executed SOW, Vendor will be solely responsible for all expenses it incurs in connection with Vendor's obligations under this Agreement. If in a SOW ASU agrees to reimburse Vendor for any travel expenses, all reimbursable travel expenses must be authorized in writing by ASU in advance of the planned travel and must be consistent with ASU Financial Services Policy FIN 421-01, www.asu.edu/aad/manuals/fin/fin421-01.html. If in a SOW ASU agrees to reimburse Vendor for any expenses, Vendor will submit all receipts and any required backup documentation to ASU within 60 days after the applicable expenses were incurred. ASU will not be required to reimburse Vendor for any expenses, invoices, or receipts for expenses received after that time. ASU will make all payments to Vendor in Vendor's legal name as set forth in the opening paragraph.

3. Term and Termination. The obligations of the parties will commence on the Effective Date and, unless sooner terminated, expire 1 year after the Effective Date (the Term). The Term may be renewed for additional periods upon written mutual agreement of both parties. The total Term will not exceed 5 years. ASU may terminate this Agreement or any SOW with or without cause upon 10 days' prior written notice to Vendor. Upon termination, ASU will have no further obligations to Vendor other than payment for Services rendered and delivered, in each case as of the effective date of termination. All provisions of this Agreement that anticipate performance after termination, and all provisions necessary to interpret and enforce them, will survive termination of this Agreement.

4. Freelancers. ASU will use Vendor's Services to procure individuals who meet ASU requirements to provide temporary services and projects to ASU (Freelancers). Due to international treaties, data security, and information transfer laws, all Freelancers must be physically present in the United States while performing services for ASU under this Agreement. At the time of engagement, each Freelancer will be required to sign a separate agreement in favor of ASU substantially in the form attached as Attachment A.

5. Independent Contractor. Vendor is an independent contractor. Neither Vendor nor any of Vendor's owners, officers, directors, managers, members, employees, agents, contractors, or subcontractors, which includes Freelancers (collectively, with Vendor, the Vendor Parties), will be employees, agents, partners, or joint venturers of ASU. The term Vendor Parties expressly includes all individuals referred by Vendor to ASU to provide freelance work to ASU (Freelancers). Where the context makes sense, references in this Agreement to Vendor include the Vendor Parties. None of the Vendor Parties will be eligible for any benefits from ASU, including worker's compensation coverage, nor will ASU make deductions from any amounts payable to Vendor for taxes. Taxes for any amounts paid to Vendor will be Vendor's sole responsibility. Vendor is responsible to ASU for the compliance with this Agreement by the Vendor Parties.

6. Hours; Business Operations. Vendor will determine Vendor's hours of work. Vendor will provide all tools, equipment, and supplies Vendor determines to be necessary to perform the Services, and Vendor will obtain and maintain in full force and effect all business registrations or licenses required to perform the Services.

7. Supervision. Vendor is using its own knowledge, skill, and technical know-how in the performance of the Services and is not being supervised by ASU. The conduct and control of Services under this Agreement lies solely with Vendor, and ASU is interested only in final results.

8. Records and Reports. Vendor will provide interim written reports concerning the performance of the Services as and when ASU may request. Upon termination of the Term, Vendor will, if requested by ASU, provide a final written report regarding the Services.

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

ASU Data will be ASU's Intellectual Property and Vendor will treat it as ASU Confidential Information. Vendor will not use, access, disclose, or license, or provide to third parties, any ASU Data, except: (i) to the extent necessary to fulfill Vendor's obligations to ASU hereunder; or (ii) as authorized in writing by ASU. Without limiting the generality of the foregoing, Vendor will not use any ASU Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, ASU's prior written consent. Vendor will not, directly or indirectly: (x) attempt to re-identify or de-aggregate deidentified or aggregated information; or (y) transfer deidentified or aggregated information to any party unless that party agrees not to attempt re-identification or de-aggregation. For ASU Data to be considered deidentified, 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 ASU, Vendor will deliver, destroy, and/or make available to ASU, any or all ASU Data.

10. Data Protection. Vendor will ensure that all Services undertaken pursuant to this Agreement are performed in compliance with applicable privacy and data protection laws, rules, and regulations, If Vendor Parties will serve as a Processor of ASU Data that includes Personal Data of Data Subjects who reside in the European Union, Vendor will cooperate with ASU to comply with the EU General Data Protection Regulation (GDPR) with respect to such Personal Data and Data Subjects. This includes ensuring that all Data Subjects have signed appropriate Consents, and signing and complying with all documents and agreements reasonably requested by ASU, including any data processing agreements. All capitalized terms in this paragraph not otherwise defined in this Agreement are defined in the GDPR.

11. Ownership and Assignment of Work Product. All Intellectual Property that any of the Vendor Parties make, conceive, discover, develop, or create, either solely or jointly with any other person or persons including ASU, specifically for or at the request of ASU in connection with the Services (the Contract IP), will be owned by ASU. To the extent any Contract IP is not considered work made for hire for ASU (or if ownership of all rights therein does not otherwise vest exclusively in ASU), Vendor hereby irrevocably assigns, and will cause the Vendor Parties to so assign, without further consideration, to ASU all right, title, and interest in and to all Contract IP, including all copyright rights of ownership. Intellectual Property means any and all inventions, designs, original works of authorship, formulas, processes, compositions, programs, databases, software, code, data, technologies, discoveries, ideas, writings, improvements, procedures, techniques, know-how, and all patent, trademark, service mark, trade secret, copyright, goodwill, and other intellectual property rights relating to the foregoing. Vendor will make full and prompt disclosure of all Contract IP to ASU. Vendor will, and will cause the Vendor Parties, upon request of ASU, do such acts, and sign such instruments to vest in ASU the entire right, title and interest to the Contract IP, and to enable ASU to prepare, file, and prosecute applications for, and to obtain patents and/or copyrights on, the Contract IP, and, at ASU's expense, to cooperate with ASU in the protection and/or defense of the Contract IP.

12. Vendor's Intellectual Property Ownership Rights. Vendor will retain ownership of its pre-existing Intellectual Property (if any), including any of its pre-existing Intellectual Property that may be incorporated into the Contract IP, provided that Vendor informs ASU in writing before incorporating any pre-existing Intellectual Property into any Contract IP. Vendor hereby grants to ASU a perpetual, irrevocable, royalty-free, worldwide right and license (with the right to sublicense), to freely use, make, have made, reproduce, disseminate, display, perform, and create derivative works based

on such pre-existing Intellectual Property as may be incorporated into the Contract IP or otherwise provided to ASU in the performance of the Services.

13. Warranties. Vendor represents and warrants that: (i) all of the Services will be performed in a professional and workmanlike manner and in conformity with industry standards by persons reasonably suited by skill, training, and experience for the type of services they are assigned to perform; (ii) Vendor will comply, and will be responsible for ensuring Vendor Parties comply, with all applicable federal, state and local laws in the performance of this Agreement; (iii) Vendor owns or has sufficient rights in all items delivered as part of the Services, and no such items or Services will infringe on or violate any Intellectual Property of any third parties; (iv) no code or software developed or delivered by Vendor Parties under this Agreement will contain any viruses, worms, Trojan Horses, or other disabling devices or code; and (v) all Services and items delivered in connection therewith will conform to the specifications and descriptions created therefor.

14. Indemnification. Vendor will indemnify, defend, and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents and employees (collectively, Indemnitee) for, from, and against any and all claims, actions, liabilities, damages, losses, or expenses (including court costs, attorneys' fees, and costs of claim processing, investigation, and litigation) for bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by (i) the negligence, acts or omissions of Vendor, or any of the other Vendor Parties; (ii) a breach of this Agreement; or (iii) failure to comply with any applicable law. Vendor will be responsible for primary loss investigation, defense and judgment costs where this indemnification is applicable.

15. Responsibility. Each party will be responsible for the negligence, acts and omissions of its employees and contractors when acting under such party's direction and supervision. Notwithstanding the terms of this Agreement or any other document or agreement: (i) other than for employees and contractors acting under ASU's direction and supervision, ASU is not responsible for any actions of any third parties, including its students; and (ii) no person may bind ASU unless they are an authorized signatory of ASU, as set forth in PUR-202, which is at www.asu.edu/counsel/manual/signatureauthority.html.

16. Limitations on Liability. NEITHER PARTY WILL HAVE ANY LIABILITY TO THE OTHER FOR ANY CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND, WHETHER IN CONTRACT, AGREEMENT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Due to the nature of the License, any loss of data is a direct damage, and not a consequential damage. ASU is a public institution and, as such, any indemnification, liability limitation, or hold harmless provision will be limited as required by Arizona law, including without limitation Article 9, Sections 5 and 7 of the Arizona Constitution and ARS §§ 35-154 and 41-621.

17. No Debarment. None of the Vendor Parties, either directly or indirectly or through subcontractors, have been suspended, excluded from participation in or penalized by any Federal or State procurement, non-procurement, or reimbursement program. Vendor affirms that it has confirmed the above statement by checking The System for Award Management (SAM) www.uscontractorregistration.com within 180 days prior to commencing Services. Vendor will provide immediate written notice to ASU upon the subsequent exclusion of any of the Vendor Parties, or upon learning of any investigation or proposed action that could result in such exclusion.

18. Notices. All notices and communications required or permitted under this Agreement will be in writing and will be given by personal delivery against receipt (including private courier service such as Federal Express), or certified United States Mail, return receipt requested. All notices and communications will be sent to the addresses set forth below or to such other address as the parties may specify in the same manner:

To ASU:
University Technology Office
PO Box
Tempe, AZ 85287-
Attn: _____

With a copy to:
ASU Purchasing and Business Services
PO Box 875212
Tempe, AZ 85287-5212
Attn: Chief Procurement Officer

To Vendor:

_____

_____

_____

Attn: _____

Notices, if delivered, and if provided in the manner set forth above, will be deemed to have been given and received on the date of actual receipt or upon the date receipt was refused. Any notice to be given by any party may be given by legal counsel for such party.

19. Nondiscrimination. The parties will comply with all applicable state and federal laws, rules, regulations, and executive orders governing equal employment opportunity, immigration, and nondiscrimination, including the Americans with Disabilities Act. **If applicable, the parties will 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.**

20. Conflict of Interest. If within 3 years after the execution of this Agreement, Vendor hires as an employee or agent any ASU representative who was significantly involved in negotiating, securing, drafting, or creating this Agreement, then ASU may cancel this Agreement as provided in Arizona Revised Statutes (ARS) § 38-511.

21. Arbitration. The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to ARS § 12-133. ARS § 12-1518 requires this provision in all ASU contracts.

22. Dispute Resolution. If a dispute arises under this Agreement, the parties will exhaust all applicable administrative remedies provided for under Arizona Board of Regents Policy 3-809.

23. Records. To the extent required by ARS § 35-214, Vendor will retain all records relating to this Agreement. Vendor will make those records available at all reasonable times for inspection and audit by ASU or the Auditor General of the State of Arizona during the term of this Agreement and for a period of five years after the completion of this Agreement. The records will be provided at Arizona State University, Tempe, Arizona, or another location designated by ASU on reasonable notice to Vendor. Records may be delivered electronically.

24. Failure of Legislature to Appropriate. In accordance with ARS § 35-154, if ASU's performance under this Agreement depends on the appropriation of funds by the Arizona Legislature, and if the Legislature fails to appropriate the funds necessary for performance, then ASU may provide written notice of this to Vendor and cancel this Agreement without further obligation of ASU. Appropriation is a legislative act and is beyond the control of ASU.

25. Weapons, Explosives, and Fireworks. ASU prohibits the use, possession, display or storage of any weapon, explosive device or fireworks on all land and buildings owned, leased, or under the control of ASU or its affiliated or related entities, in all ASU residential facilities (whether managed by ASU or another entity), in all ASU vehicles, and at all ASU or ASU affiliate sponsored events and activities, except as provided in ARS § 12-781, or unless written permission is given by the Chief of the ASU Police Department or a designated representative. Notification by Vendor to all persons or entities who are employees, officers, subcontractors, consultants, Freelancers agents, guests, invitees or licensees of Vendor (Vendor Notification Parties) of this policy is a condition and requirement of this Agreement. Vendor further agrees to enforce this requirement against all Vendor Notification Parties. ASU's policy may be accessed at: www.asu.edu/aad/manuals/pdp/pdp201-05.html.

26. Advertising, Publicity, Names and Marks. Vendor will not do any of the following, without, in each case, ASU's prior written consent: (i) use any names, service marks, trademarks, trade names, logos, or other identifying names, domain names, or identifying marks of ASU (ASU Marks), for any reason including online, advertising, or promotional purposes; (ii) issue a press release or public statement regarding this Agreement; or (iii) represent or imply any ASU endorsement or support of any product or service in any public or private communication. Any permitted use of any ASU Marks must comply with ASU's requirements, including using the ® indication of a registered trademark where applicable.

27. Information Security. All systems containing ASU Data must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable federal and state laws, regulations and policies. To

diminish information security threats, Vendor will (either directly or through its third party service providers) meet the requirements set forth on Exhibit B.

28. Background Checks. Vendor will, at Vendor's expense, conduct reference checks, and employment, education, SSN trace, National Sex Offender Registry, and criminal history record checks (collectively, Screenings) on those persons employed or contracted (including Freelancers) by Vendor for security or safety-sensitive positions, as defined in ASU ACD 126, or who may have access to sensitive or highly sensitive ASU data, as defined ASU's Data Handling Standard. Vendor will conduct all Screenings within 90 days prior to a person commencing work under this Agreement. Vendor will exclude from any direct participation in Vendor's performance under this Agreement, any unqualified persons. Vendor will maintain, as part of the records Vendor is required to maintain hereunder, all Screening information and all documentation relating to work performance for each employee or contractor who performs work hereunder. Vendor will abide by all applicable laws, rules and regulations, including the Fair Credit Reporting Act, and equal opportunity laws, rules, and regulations.

29. Americans with Disabilities Act and Rehabilitation Act. Vendor will comply with all applicable provisions of the Americans with Disabilities Act, the Rehabilitation Act of 1973, and all applicable federal regulations, as amended from time to time (ADA Laws). All electronic and information technology and products and services to be used by ASU faculty/staff, students, program participants, or other ASU constituencies must be compliant with the ADA Laws. 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.

30. Insurance Requirements. Without limiting any liabilities or any other obligation of Vendor, Vendor will purchase and maintain (and cause its subcontractors to purchase and maintain), until all of their obligations have been discharged, including any warranty periods under this Agreement, or are satisfied, insurance against claims for injury to persons or damage to property that may arise from or in connection with the performance of the work hereunder by Vendor, its agents, representatives, employees or subcontractors as described on Exhibit C.

31. Privacy; Educational Records. Student educational records are protected by the U.S. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA). Entity will not require any ASU students or employees to waive any privacy rights (including under FERPA or the GDPR) as a condition for receipt of any educational services, and any attempt to do so will be void. Entity will comply with FERPA and will not access or make any disclosures of student educational records to third parties without prior notice to and consent from ASU or as otherwise provided by law. If this Agreement contains a scope of work or other provision that requires or permits Entity to access or release any student records, then, for purposes of this Agreement only, ASU designates Entity as a "school official" for ASU under FERPA, as that term is used in FERPA and its implementing regulations. In addition, any access or disclosures of student educational records made by Entity or any Entity Parties must comply with ASU's definition of legitimate educational purpose in SSM 107-01: Release of Student Information. If Entity violates the terms of this section, Entity will immediately provide notice of the violation to ASU.

32. Title IX Obligation. Title IX protects individuals from discrimination based on sex, including sexual harassment. ASU fosters a learning and working environment that is built on respect and free of sexual harassment. ASU's Title IX Guidance is available at www.asu.edu/titleIX/Vendors-and-an-Environment-of-Respect.pdf. Vendor will: (i) comply with ASU's Title IX Guidance; (ii) provide ASU's Title IX Guidance to any Vendor Parties who may reasonably be expected to interact with ASU students and employees, in person or online; and (iii) ensure that all Vendor Parties comply with ASU's Title IX Guidance.

33. Authorized Presence Requirements. As required by ARS § 41-4401, ASU is prohibited from awarding a contract to any contractor or subcontractor that fails to comply with ARS § 23-214(A) (verification of employee eligibility through the e-verify program). Vendor warrants that it and its subcontractors comply fully with all applicable federal immigration laws and regulations that relate to their employees and their compliance with ARS § 23-214(A). A breach of this warranty will be a material breach of this Agreement that is subject to penalties up to and including termination of this Agreement. ASU retains the legal right to inspect the papers of any Contractor or subcontractor employee who works hereunder to ensure that the contractor or subcontractor is complying with the above warranty.

34. Leased Employees. Vendor will determine and inform ASU if any leased employees are retired members of the Arizona State Retirement System prior to the leased employee performing any work under this Agreement.

35. Tobacco-Free University. ASU is tobacco free. For details, visit www.asu.edu/tobaccofree.

36. Offshore Performance of Work Prohibited. Due to security and identification protection concerns, direct Services under this Agreement will be performed within the borders of the United States. Any Services that are described in any

SOW that directly serve ASU and may involve access to secure or sensitive data or personal client data or development or modification of software for ASU will be performed within the borders of the United States. Unless stated otherwise in the scope of work, this definition 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.

37. Construction. Each party acknowledges that it has had the opportunity to participate in the drafting of, and to have its legal counsel review, this Agreement. Vendor is not relying on the advice or counsel of any individuals employed by ASU in entering into this Agreement. Any rule of construction to the effect that any ambiguities are to be resolved against the drafting party will not be applied in interpreting this Agreement.

38. Americans with Disabilities and Rehabilitation Acts. Vendor Parties will comply with all applicable provisions of the Americans with Disabilities Act, the Rehabilitation Act of 1973, and all applicable federal regulations. All electronic and information technology and products and services to be used by ASU faculty/staff, students, program participants, or other ASU constituencies must be compliant with the Americans with Disabilities Act and Section 508 of the Rehabilitation Act of 1973, as amended from time to time. 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.

39. No Boycott of Israel. As required by ARS §§ 35-393 to 35-393.01, Vendor certifies it is not currently engaged in a boycott of Israel and will not engage in a boycott of Israel during the term of this Agreement.

40. Governing Law and Venue. This Agreement will be governed by the laws of the State of Arizona without regard to any conflicts of laws principles. ASU's obligations hereunder are subject to the regulations/policies of the Arizona Board of Regents. Any proceeding arising out of or relating to this Agreement will be conducted in Maricopa County, Arizona. Each party waives any objection it may now or hereafter have to venue or to convenience of forum.

41. Essence of Time. Time is of the essence in the performance of this Agreement.

The parties have signed this Agreement as of the Effective Date.

Arizona Board of Regents for and on behalf of Arizona State University	**Vendor:**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____

EXHIBIT A – SERVICES, DELIVERABLES, AND CONSIDERATION

EXHIBIT B – INFORMATION SECURITY

All systems containing ASU Data must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable federal and state laws, regulations and policies. To diminish information security threats, Vendor will (either directly or through its third party service providers) meet the following requirements. Sections (a) through (f) apply in all cases, Sections (g) through (j) apply to the extent Vendor (i) is creating any code for ASU, (ii) receives, stores, or analyzes ASU Data (including if the data is not online), or (iii) is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data.

(a) Access Control. Control access to ASU's resources, including sensitive ASU Data, limiting access to legitimate business need based on an individual's job-related assignment. Vendor will, or will cause the system administrator to, approve and track access to ensure proper usage and accountability, and Vendor will make such information available to ASU for review, upon ASU's request.

(b) Incident Reporting. Report information security incidents immediately to ASU (including those that involve information disclosure incidents, unauthorized disclosure of ASU Data, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities).

(c) Off Shore. Direct services under this Agreement will be performed within the borders of the United States. Any services that are described in this Agreement that directly serve ASU and may involve access to secure or sensitive ASU Data or personal client data or development or modification of software for ASU will be performed within the borders of the United States. 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 ASU Data.

(d) Patch Management. Carry out updates and patch management for all systems and devices in a timely manner and to the satisfaction of ASU. Updates and patch management must be deployed using an auditable process that can be reviewed by ASU upon ASU's request.

(e) Encryption. All systems and devices that store, process or transmit sensitive ASU Data must use an industry standard encryption protocol for data in transit and at rest.

(f) Notifications. Notify ASU immediately if Vendor receives any kind of subpoena for or involving ASU Data, if any third-party requests ASU Data, or if Vendor has a change in the location or transmission of ASU Data. All notifications to ASU required in this Information Security paragraph will be sent to ASU Information Security at Infosec@asu.edu, in addition to any other notice addresses in this Agreement.

(g) Security Reviews. Complete SOC2 Type II or substantially equivalent reviews in accordance with industry standards, which reviews are subject to review by ASU upon ASU's request. Currently, no more than two reviews per year are required.

(h) Scanning and Penetration Tests. Perform periodic scans, including penetration tests, for unauthorized applications, services, code and system vulnerabilities on the networks and systems included in this Agreement in accordance with industry standards and ASU standards (as documented in NIST 800-115) or equivalent. All web based applications (e.g., HTTP/HTTPS accessible URLs, APIs, and web services) are required to have their own web application security scan and remediation plan. Vendor must correct weaknesses within a reasonable period of time, and Vendor must provide proof of testing to ASU upon ASU's request.

(i) ASU Rights. ASU reserves the right (either directly or through third party service providers) to scan and/or penetration test any purchased and/or leased software regardless of where it resides.

(j) Secure Development. Use secure development and coding standards including secure change management procedures in accordance with industry standards. Perform penetration testing and/or scanning prior to releasing

new software versions. Vendor will provide internal standards and procedures to ASU for review upon ASU request.

EXHIBIT C
INSURANCE REQUIREMENTS

Without limiting any liabilities or any other obligation of Vendor, Entity will purchase and maintain (and cause its subcontractors to purchase and maintain), until all of their obligations have been discharged or satisfied, including any warranty periods under this Agreement, insurance against claims that may arise from or in connection with the performance of the work hereunder by Entity, its agents, representatives, employees or subcontractors, as described in this Exhibit C.

These insurance requirements are minimum requirements for this Agreement and in no way limit any indemnity covenants in this Agreement. ASU does not warrant that these minimum limits are sufficient to protect Entity from liabilities that might arise out of the performance of the work under this Agreement by Entity, its agents, representatives, employees, or subcontractors. These insurance requirements may change if Vendor is a foreign entity, or with foreign insurance coverage.

A. **Minimum Scope and Limits of Insurance**: Entity's insurance coverage will be primary insurance with respect to all other available sources. Entity will provide coverage with limits of liability not less than those stated below:

1. Commercial General Liability – Occurrence Form. Policy will include bodily injury, property damage, personal injury, and broad form contractual liability coverage.

● General Aggregate	$2,000,000
● Product - Completed Operations Aggregate	$1,000,000
● Personal and Advertising Injury	$1,000,000
● Contractual Liability	$1,000,000
● Fire Legal Liability (only if Agreement is for leasing space)	$ 50,000
● Each Occurrence	$1,000,000

a. Policy will include the following additional insured language: "The State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, will be named as additional insureds with respect to liability arising out of the activities performed by or on behalf of Entity."

b. Policy will contain a waiver of subrogation against the State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, for losses arising from work performed by or on behalf of Entity.

2. Worker's Compensation and Employers' Liability. Applicable statutory limits, as amended from time to time.

a. Employer's Liability in the amount of $1 million injury and disease.

b. Policy will contain a waiver of subrogation against the State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, for losses arising from work performed by or on behalf of Entity.

c. This requirement will not apply to any contractor or subcontractor exempt under ARS § 23-901, when such contractor or subcontractor signs the appropriate waiver (Sole Proprietor/Independent Contractor) form.

4. Technology/Network Errors and Omissions Insurance.

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

a. This insurance will cover Entity's liability for acts, errors and omissions arising out of Entity'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 this Agreement is written on a claims-made basis, Entity warrants that any retroactive date under the policy will precede the effective date of this 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 this Agreement is completed.

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

5. Professional Liability (Errors and Omissions Liability)**.**

- Each Claim $1,000,000
- Annual Aggregate $2,000,000

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

b. Policy will cover professional misconduct for those positions defined in the scope of work of this Agreement.

B. Cancellation; Material Changes: Cancellation notices will be delivered to ASU in accordance with all policy provisions. Notices required in this Section must be sent directly to ASU Director of Risk Management, PO Box 876512, Tempe, AZ, 85287-6512 and will be sent by U.S. certified mail, return receipt requested.

C. Acceptability of Insurers: Insurance is to be placed with duly licensed or approved non-admitted insurers in the State of Arizona with an "A.M. Best" rating of not less than A- VII. ASU in no way warrants that the above required minimum insurer rating is sufficient to protect Entity from potential insurer insolvency. Self-Insurance may be accepted in lieu of or in combination with insurance coverage requested.

D. Verification of Coverage: Entity will furnish ASU with valid certificates of insurance as required by this Agreement. All valid certificates evidencing insurance required by this Agreement are to be received and approved by ASU before work commences. Each insurance policy required by this Agreement must be in effect at or prior to commencement of work under this Agreement and remain in effect for the term of this Agreement. Failure to maintain the insurance policies as required by this Agreement, or to provide evidence of renewal, is a material breach of contract.

All certificates required by this Section must be sent to ASU Director of Risk Management, PO Box 876512, Tempe, AZ, 85287-6512. ASU's project or purchase order number and project description will be noted on

each certificate of insurance. The State of Arizona and ASU may require complete, certified copies of policies at the time of notice of any loss or claim.

E. Subcontractors. Entity's certificate(s) may include all subcontractors as insureds under its policies as required by this Agreement, or Entity will furnish to ASU copies of valid certificates and endorsements for each subcontractor. Coverages for subcontractors will be subject to the minimum requirements identified above.

F. Approval. These insurance requirements are the standard insurance requirements of ASU. Any modification or variation from the insurance requirements in this Agreement will require the approval of ASU's Department of Risk and Emergency Management.

ATTACHMENT A
ASU FREELANCER AGREEMENT

In consideration of the engagement by the Arizona Board of Regents for and on behalf of Arizona State University (ASU) of the undersigned individual (Freelancer) as an independent contractor, to perform the services on detailed on a Statement of Work Exhibit A (the Services), and the fees to be received by Freelancer, Freelancer agrees as follows:

1. Assignment. Freelancer hereby irrevocably assigns to ASU all right, title and interest in and to all Intellectual Property that Freelancer makes, conceives, discovers, develops, or creates, either solely or jointly with any other person or persons including ASU, for or at the request of ASU in connection with the Services (Freelance IP). Intellectual Property means any and all inventions, designs, original works of authorship, formulas, processes, compositions, programs, databases, data, technologies, discoveries, ideas, writings, improvements, procedures, techniques, know-how, and all patent, trademark, service mark, trade secret, copyright and other intellectual property rights (and goodwill) relating to the foregoing. As and when reasonably requested by ASU, at ASU's expense, Freelancer will do such things, and sign such documents to vest in ASU the right, title and interest to the Freelance IP, and to enable ASU to prepare and file, and obtain patents and/or copyrights on, and to otherwise protect and defend, the Freelance IP. If Freelancer is a resident of California, the provisions on Exhibit B apply.

2. Confidentiality. All Intellectual Property, Freelance IP, and other information regarding ASU that ASU provides to Freelancer or Freelancer develops or has access to during the engagement with ASU (Information) is proprietary and confidential information of ASU, and the unauthorized disclosure of Information by Freelancer could result in irreparable damage to ASU, which damage would be difficult to quantify. Freelancer will not use any Information for any purpose other than providing the Services to ASU. Freelancer will not transfer originals or copies of Information to any third party without ASU's prior written consent. All Information will remain the property of ASU. Freelancer will immediately return all Information to ASU upon ASU's written request. Freelancer has no obligation to maintain confidential any Information that Freelancer can show: (a) is already lawfully in the possession of or known by Freelancer before the Information was received from ASU; (b) is or becomes generally known in the industry through no violation of this Agreement; (c) is lawfully received by Freelancer from any third party without restriction on disclosure or use; (d) is independently developed without violating this Agreement; or (e) is required to be disclosed by court order following notice sufficient to allow ASU to contest such order.

3. Warranties. Freelancer warrants to ASU that: (i) Freelancer will perform the Services in a professional manner in compliance with industry standards and all applicable laws, rules, and regulations, including applicable data protection and privacy laws; (ii) any software, Services, deliverables, or Intellectual Property, developed or delivered under this Agreement will not infringe any Intellectual Property or other rights of any third party, and will not contain any viruses, worms, Trojan Horses, or other disabling devices or code.

4. Independent Contractor; No Benefits. Freelancer's is an independent contractor of ASU. Freelancer is and will not be an employee or agent of ASU. Neither ASU nor Freelancer will have any authority to act on behalf of or to bind the other. Freelancer will not be entitled to Workers Compensation coverage or any other benefits covering ASU employees. ASU will not be responsible for paying payroll or withholding taxes, or FICA, or similar payments, to any government agencies for or on behalf of Freelancer.

5. Conflict of Interest. If within 3 years after the execution of this Agreement, Freelancer hires as an employee or agent any ASU representative who was significantly involved in negotiating, securing, drafting, or creating this Agreement, then ASU may cancel this Agreement as provided in Arizona Revised Statutes (ARS) § 38-511.

6. Dispute Resolution. If a dispute arises under this Agreement, Freelancer will exhaust all applicable administrative remedies under Arizona Board of Regents Policy 3-809. Freelancer agrees to arbitrate those disputes that may be filed in Arizona Superior Court and that are subject to mandatory arbitration pursuant to ARS § 12-133.

7. Records. To the extent required by ARS § 35-214, Freelancer will retain all records relating to this Agreement. Freelancer will make those records available at all reasonable times for inspection and audit by ASU or the Auditor General of the State of Arizona during the term of this Agreement and for 5 years after the completion of this Agreement. The records will be provided at ASU in Tempe, Arizona, or another location designated by ASU on reasonable notice to Freelancer.

8. Term. The term of Freelancer's engagement by ASU will end on the sooner of: (i) the completion of the Services; (ii) the Completion Date on Exhibit A; or (iii) 30 days after ASU sends notice of termination to Freelancer at Freelancer's Notice Address below. On termination ASU will have no obligations to Freelancer other than payment for Services rendered. The term will not exceed 5 years.

9. ASU Terms of Use and Privacy Policy. Freelancer will comply with ASU's Privacy Policy and Terms of Use as set forth in the links at the bottom of each ASU.edu webpage.

10. Assignment. Freelancer may not transfer or assign any of his or her obligations under this Agreement, either directly or indirectly. Freelancer may not engage any other individuals or entities to perform any of the Services.

11. Governing Law; Venue. This Agreement will be governed by the laws of the State of Arizona. Any proceeding arising out of or relating to this Agreement will be conducted in Maricopa County, Arizona. Freelancer consents to such jurisdiction, and waives any objection it may have to venue or convenience of forum.

Freelancer Acknowledgement: I have read and fully understand my obligations under this Agreement. I have not relied on any statements or advice of ASU or any of its employees in deciding to sign this Agreement, and I have had the opportunity to have this Agreement reviewed and explained to me by my own advisors.

Freelancer Signature: _____ Date Signed: _____

Freelancer Legal Name: _____

Notice Address: _____

_____

Freelancer Email: _____

ASU Contact/Sponsor Department: _____

ASU Responsible Individual Name: _____ Email: _____

Exhibit A – Statement of Work

Exhibit B – California Labor Code Notice – Applied when Freelancer is a California Resident

EXHIBIT A

STATEMENT OF WORK NO. ____
Freelancer:
Department:
Project:

This Statement of Work is made in accordance with the ASU Freelancer Agreement between _____ (Freelancer) and the Arizona Board of Regents for and on behalf of Arizona State University (ASU), dated _____ (the Agreement). To the extent any provision in this Statement of Work conflicts with any provisions of the Agreement, the provisions of the Agreement will control.

PROJECT DESCRIPTION:

FREELANCER RESPONSIBILITIES:

DELIVERABLES:

TERM & TIMELINES:
· Completion Date:

FEES:

Arizona Board of Regents for and
on behalf of Arizona State University

By: _____
Name: _____
Title: _____
Date Signed: _____

_____.:

By: _____
Name: _____
Title:_____
Date Signed: _____

EXHIBIT B

California Labor Code Section 2870 Notice

To the extent this Agreement is deemed to be subject to Section 2870 of the California Labor Code, Freelancer acknowledges and understands that, notwithstanding anything herein to the contrary, nothing in this Agreement will be deemed to require Freelancer to assign or offer to assign any of Freelancer's rights to ASU in any invention that qualifies fully under Section 2870, which states as follows:

(a) ANY PROVISION IN AN EMPLOYMENT AGREEMENT WHICH PROVIDES THAT AN EMPLOYEE WILL ASSIGN, OR OFFER TO ASSIGN, ANY OF HIS OR HER RIGHTS IN AN INVENTION TO HIS OR HER EMPLOYER WILL NOT APPLY TO AN INVENTION THAT THE EMPLOYEE DEVELOPED ENTIRELY ON HIS OR HER OWN TIME WITHOUT USING THE EMPLOYER'S EQUIPMENT, SUPPLIES, FACILITIES, OR TRADE SECRET INFORMATION EXCEPT FOR THOSE INVENTIONS THAT EITHER: (1) RELATE AT THE TIME OF CONCEPTION OR REDUCTION TO PRACTICE OF THE INVENTION TO THE EMPLOYER'S BUSINESS, OR ACTUAL OR DEMONSTRABLY ANTICIPATED RESEARCH OR DEVELOPMENT OF THE EMPLOYER; OR (2) RESULT FROM ANY WORK PERFORMED BY THE EMPLOYEE FOR THE EMPLOYER.

(b) TO THE EXTENT A PROVISION IN AN EMPLOYMENT AGREEMENT PURPORTS TO REQUIRE AN EMPLOYEE TO ASSIGN AN INVENTION OTHERWISE EXCLUDED FROM BEING REQUIRED TO BE ASSIGNED UNDER SUBDIVISION (a), THE PROVISION IS AGAINST THE PUBLIC POLICY OF THIS STATE AND IS UNENFORCEABLE.

Any disclosures by Freelancer to ASU of any invention that qualifies fully under Section 2870 will be received in confidence.

SECTION XIII – MANDATORY CERTIFICATIONS

(Fillable PDF versions of mandatory certifications are located on-line under Supplier Forms: http://cfo.asu.edu/purchasing-forms. ORIGINAL signatures are REQUIRED for either version.)

CONFLICT OF INTEREST CERTIFICATION

_____
(Date)

Purchasing and Business Services
Arizona State University
PO Box 875212
Tempe, AZ 85287-5212

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

( ) There is no officer or employee of Arizona State University who has, or whose relative has, a substantial interest in any contract resulting from this request.

( ) The names of any and all public officers or employees of Arizona State University who have, or whose relative has, a substantial interest in any contract resulting from this request, and the nature of the substantial interest, are included below or as an attachment to this certification.

_____ _____
(Firm) (Address)

_____ _____
(Email Address)

_____ _____
(Signature required) (Phone)

_____ _____
(Print name) (Fax)

_____ _____
(Print title) (Federal Taxpayer ID Number)

(Purchasing 1/31/07. Previous editions are obsolete and cannot be used.)

FEDERAL DEBARRED LIST CERTIFICATION

Certification Regarding Debarment, Suspension, Proposed Debarment, and Other Responsibility Matters (Dec 2001)

_____
(Date)

Purchasing and Business Services
Arizona State University
PO Box 875212
Tempe, AZ 85287-5212

In accordance with the Federal Acquisition Regulation, 52.209-5:

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—
(i) The Offeror and/or any of its Principals—

(A) (check one) **Are ( )** or **are not ( )** presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency; (The debarred list (List of Parties Excluded from Federal Procurement and Non-Procurement Programs) can be found at https://www.sam.gov/index.html/.)

(B) (check one) **Have ( )** or **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) (check one) **Are ( )** or **are not ( )** presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision.

(ii) The Offeror (check one) **has ( )** or **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.

_____	_____
(Firm)	(Address)
_____	_____
(Email Address)	
_____	_____
(Signature required)	(Phone)
_____	_____
(Print name)	(Fax)
_____	_____
(Print title)	(Federal Taxpayer ID Number)

(Federal Debarred List Continued)
(Purchasing 1/31/07)

ANTI-LOBBYING CERTIFICATION

Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (Sept 2007)

_____
(Date)

Purchasing and Business Services
Arizona State University
PO Box 875212
Tempe, AZ 85287-5212

In accordance with the Federal Acquisition Regulation, 52.203-11:

(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 this contract;

(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 an 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.

(Signature page follows)

_____	_____
(Firm)	(Address)
_____	_____
(Email Address)	
_____	_____
(Signature required)	(Phone)
_____	_____
(Print name)	(Fax)
_____	_____
(Print title)	(Federal Taxpayer ID Number)

(Anti-Lobbying Certificate)
(Purchasing 1/31/07)

LEGAL WORKER CERTIFICATION

_____
(Date)

Purchasing and Business Services
Arizona State University
PO Box 875212
Tempe, AZ 85287-5212

Authorized Presence Requirements. As required by ARS § 41-4401, ASU is prohibited from awarding a contract to any contractor or subcontractor that fails to comply with ARS § 23-214(A) (verification of employee eligibility through the e-verify program). Vendor warrants that it and its subcontractors comply fully with all applicable federal immigration laws and regulations that relate to their employees and their compliance with ARS § 23-214(A). A breach of this warranty will be a material breach of this Contract that is subject to penalties up to and including termination of this Contract ASU retains the legal right to inspect the papers of any Contractor or subcontractor employee who works hereunder to ensure that the contractor or subcontractor is complying with the above warranty.

A breach of the foregoing warranty shall be deemed a material breach of the contract. In addition to the legal rights and remedies available to the University hereunder and under the common law, in the event of such a breach, the University shall have the right to terminate the contract. Upon request, the University shall have the right to inspect the papers of each contractor, subcontractor or any employee of either who performs work hereunder for the purpose of ensuring that the contractor or subcontractor is in compliance with the warranty set forth in this provision.

_____ (Firm)	_____ (Address)
_____ (Email address)	_____
_____ (Signature required)	_____ (Phone)
_____ (Print name)	_____ (Fax)
_____ (Print title)	_____ (Federal Taxpayer ID Number)

(Purchasing 7/25/16)

Voluntary Product Accessibility Template (VPAT)

All electronic and information technology developed, procured, maintained, or used in carrying out University programs and activities must be compliant with Sections 504 and 508 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, as amended, other relevant local, state, and federal laws, and related university policies.

This VPAT was designed to provide information on how a product or service conforms to the section 508 accessibility standards (from the U.S. Access Board) for electronic and information technology (EIT) in a consistent fashion and format. Supplier must make specific statements, in simple understandable language, about how their product or service meets the requirements of the section 508 standards.

SUPPLIER MUST COMPLETE ALL SECTIONS.

DATE:	
PRODUCT NAME:	
PRODUCT VERSION NUMBER:	
SUPPLIER COMPANY NAME:	
SUPPLIER CONTACT NAME:	
SUPPLIER CONTACT EMAIL:	

SUMMARY TABLE		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
Section 1194.21 Software Applications and Operating Systems		
Section 1194.22 Web-based Internet Information and Applications		
Section 1194.23 Telecommunications Products		
Section 1194.24 Video and Multi-media Products		
Section 1194.25 Self-Contained, Closed Products		
Section 1194.26 Desktop and Portable Computers		
Section 1194.31 Functional Performance Criteria		
Section 1194.41 Information, Documentation and Support		

Section 1194.21 Software Applications and Operating Systems - Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) When software is designed to run on a system that has a keyboard, product functions shall be		

executable from a keyboard where the function itself or the result of performing a function can be discerned textually.		
(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.		
(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.		
(d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text.		
(e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.		
(f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.		
(g) Applications shall not override user selected contrast and color selections and other individual display attributes.		
(h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.		
(i) Color coding shall not be used as the only means of conveying information, indicating an action,		

prompting a response, or distinguishing a visual element.		
(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.		
(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.		
(l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.		

Section 1194.22 Web-based Intranet and Internet information and Applications - Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).		
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.		
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.		
(d) Documents shall be organized so they are readable without requiring an associated style sheet.		
(e) Redundant text links shall be provided for each active region of a server-side image map.		
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.		
(g) Row and column headers shall be identified for data tables.		
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.		

(i) Frames shall be titled with text that facilitates frame identification and navigation		
(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.		
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.		
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.		
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with 1194.21(a) through (l).		
(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.		
(o) A method shall be provided that permits users to skip repetitive navigation links.		
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.		

Section 1194.23 Telecommunications Products - Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and		

off to allow the user to intermix speech with TTY use.		
(b) Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.		
(c) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.		
(d) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.		
(e) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.		
(f) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.		
(g) If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use.		
(h) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.		
(i) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.		
(j) Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols,		

formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.		
(k)(1) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be tactilely discernible without activating the controls or keys.		
(k)(2) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be operable with one hand and shall not require tight grasping, pinching, twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2N) maximum.		
(k)(3) Products which have mechanically operated controls or keys shall comply with the following: If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.		
(k)(4) Products which have mechanically operated controls or keys shall comply with the following: The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.		

Section 1194.24 Video and Multi-media Products – Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. Widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes		

DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.		
(b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.		
(c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned.		
(d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.		
(e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.		

Section 1194.25 Self-Contained, Closed Products – Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) Self-contained products shall be usable by people with disabilities without requiring an end-user to attach Assistive Technology to the product. Personal headsets for private listening are not Assistive Technology.		
(b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.		
(c) Where a product utilizes touchscreens or contact-sensitive controls, an input method shall be provided that complies with 1194.23 (k) (1) through (4).		
(d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.		
(e) When products provide auditory output, the audio signal shall be		

provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at any time.		
(f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.		
(g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.		
(h) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.		
(i) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.		
(j) (1) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length on products which are freestanding, non-portable, and intended to be used in one location and which have operable controls.		
(j)(2) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.		
(j)(3) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is more than 10 inches and not more than		

24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.		
(j)(4) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Operable controls shall not be more than 24 inches behind the reference plane.		

Section 1194.26 Desktop and Portable Computers – Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) All mechanically operated controls and keys shall comply with 1194.23 (k) (1) through (4).		
(b) If a product utilizes touchscreens or touch-operated controls, an input method shall be provided that complies with 1194.23 (k) (1) through (4).		
(c) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.		
(d) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards		

Section 1194.31 Functional Performance Criteria – Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.		
(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.		

(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided		
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.		
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.		
(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.		

Section 1194.41 Information, Documentation and Support – Detail		
Criteria	**Level of Support & Supporting Features**	**Remarks and Explanations**
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge		
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.		
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.		

USE THE FOLLOWING LANGUAGE FOR FILLING OUT THE LEVEL OF SUPPORT AND SUPPORTING FEATURES COLUMN IN THE TABLES ABOVE.

SUPPORTS - Use this language when you determine the product fully meets the letter and intent of the Criteria.

SUPPORTS WITH EXCEPTIONS - Use this language when you determine the product does not fully meet the letter and intent of the Criteria, but provides some level of access relative to the Criteria.

SUPPORTS THROUGH EQUIVALENT FACILITATION - Use this language when you have identified an alternate way to meet the intent of the Criteria or when the product does not fully meet the intent of the Criteria.

SUPPORTS WHEN COMBINED WITH COMPATIBLE AT - Use this language when you determine the product fully meets the letter and intent of the Criteria when used in combination with compatible assistive technology. For example, many software programs can provide speech output when combined with a compatible screen reader (commonly used assistive technology for people who are blind).

DOES NOT SUPPORT - Use this language when you determine the product does not meet the letter or intent of the Criteria.

NOT APPLICABLE - Use this language when you determine that the Criteria do not apply to the specific product.

NOT APPLICABLE - FUNDAMENTAL ALTERATION EXCEPTION APPLIES - Use this language when you determine a fundamental alteration of the product would be required to meet the criteria. “Fundamental alteration” means a change in the fundamental characteristic or purpose of the product or service, not merely a cosmetic or aesthetic change. Generally, adding access should not change the basic purpose or characteristics of a product in a fundamental way.

The Supplier Sustainability Questionnaire is used to help the University understand how sustainable a supplier is. Sustainability is an important goal for the University, and as such, we expect our suppliers to help us support this goal. There are two (2) different questionnaires posted, one is for large companies while the other is for small businesses. A company is considered to be large when there are more than 100 full-time employees or over 4 million dollars in annual revenue generated.

SUPPLIER SUSTAINABILITY QUESTIONNAIRE – LARGE COMPANY

Firm Name: _____ Date: _____

The Supplier Sustainability Questionnaire must be completed and returned with your Proposal. This questionnaire is applicable to firms that provide services as well as those that provide goods.

The University's vision is to be environmentally sustainable while expanding our education, research, and community support programs. The University seeks suppliers who share our sustainability vision. Accordingly, please answer the following questions.

To each question please provide at least one (1) of the following types of responses:

- An explanation or description
- A URL of your policy or program

An electronic copy of your illustrative policies or programs must be provided if requested. If the question does not apply, answer with N/A and provide an explanation as to why.

Energy

1. What is your firm doing to be energy efficient?
2. What are your firm's annual greenhouse gas emissions in metric tons of carbon dioxide equivalent? (Enter total metric tons of CO2 equivalency [includes the following GHGs: CO2, CH4, N2), SF6, HFCs and PFCs])
3. What plan is in place to reduce greenhouse gas emissions in the future?

Solid Waste

1. What is your firm doing to reduce waste to landfill?
2. What is your firm's annual waste to landfill generated in metric tons? (Enter total metric tons)
3. What plan is in place to reduce waste to landfill generated in the future?

Water Waste

1. What is your firm doing to reduce water waste?
2. What is your firm's annual water waste in gallons? (Enter total gallons)
3. What plan is in place to reduce water waste in the future?

Packaging

1. What is your firm's plan to minimize packaging and/or describe your firm's packaging "Take Back" program?
2. What kind of reusable, recyclable, and/or compostable packaging materials does your firm use?
3. What does your firm do to encourage/require your suppliers to minimize packaging and/or use reusable, recyclable, or compostable packaging materials?

Sustainability Practices

1. What programs does your firm have to encourage your employees to use alternative transportation while commuting to work and travelling locally?
2. What sustainability guidelines or environmental statement does your firm have to guide the firm as a whole?
3. What are your firm's sustainable purchasing guidelines?
4. What kind of position(s) or team(s) does your firm have dedicated to overseeing sustainability initiatives?
5. List the sustainability related professional associations of which your firm is a member.
6. What kind of effort does your firm make to reduce the use of environmentally harmful materials?
7. Has an environmental life-cycle analysis of your firm's products been conducted by a certified testing organization?
8. Does your firm use Green Seal/EcoLogo certified or biodegradable/eco-friendly cleaning products?
9. Has your firm been cited for non-compliance of an environmental or safety issue in the past ten years?
10. Name any third party certifications your firm has in regards to sustainable business practices?
11. Describe any other initiatives your firm has taken to integrate sustainability practices principles into your operations.

Community

1. What charity, community development, educational programs, or environmental programs is your firm involved in within your local community?
2. What educational programs does your firm have to develop employees?

SUPPLIER SUSTAINABILITY QUESTIONNAIRE – SMALL COMPANY

Firm Name: _____ Date: _____

The Supplier Sustainability Questionnaire must be completed and returned with your Proposal. This questionnaire is applicable to firms that provide services as well as those that provide goods.

The University's vision is to be environmentally sustainable while expanding our education, research, and community support programs. The University seeks suppliers who share our sustainability vision. Accordingly, please answer the following questions.

To each question please provide at least one (1) of the following types of responses:

- An explanation or description
- A URL of your policy or program

An electronic copy of your illustrative policies or programs must be provided if requested. If the question does not apply, answer with N/A and provide an explanation as to why.

Energy

1. What is your firm doing to be energy efficient?
2. What plan is in place to reduce greenhouse gas emissions in the future?

Solid Waste

1. What is your firm doing to reduce waste to landfill?
2. What plan is in place to reduce waste to landfill generated in the future?

Water Waste

1. What is your firm doing to reduce water waste?
2. What plan is in place to reduce water waste in the future?

Packaging

1. What is your firm's plan to minimize packaging and/or describe your firm's packaging "Take Back" program?
2. What kind of reusable, recyclable, and/or compostable packaging materials does your firm use?
3. What does your firm do to encourage/require your suppliers to minimize packaging and/or use reusable, recyclable, or compostable packaging materials?

Sustainability Practices

1. What programs does your firm have to encourage your employees to use alternative transportation while commuting to work and travelling locally?
2. What sustainability guidelines or environmental statement does your firm have to guide the firm as a whole?
3. What are your firm's sustainable purchasing guidelines?
4. What kind of position(s) or team(s) does your firm have dedicated to overseeing sustainability initiatives?
5. List the sustainability related professional associations of which your firm is a member.
6. What kind of effort does your firm make to reduce the use of environmentally harmful materials?
7. Does your firm use Green Seal/EcoLogo certified or biodegradable/eco-friendly cleaning products?
8. Has your firm been cited for non-compliance of an environmental or safety issue in the past ten years?

9. Name any third party certifications your firm has in regards to sustainable business practices?
10. Describe any other initiatives your firm has taken to integrate sustainability practices principles into your operations.

Community

1. What charity, community development, educational programs, or environmental programs is your firm involved in within your local community?
2. What educational programs does your firm have to develop employees?

If your firm is just beginning the sustainability journey, or is looking for tools and resources, here are some suggestions:

Energy

Greenhouse Gas Protocol provides tools to calculate emissions that are industry specific:
- http://www.ghgprotocol.org/calculation-tools

Practice Green health provides basic information and tools for emissions as well:
- https://practicegreenhealth.org/topics/energy-water-and-climate/climate/tracking-and-measuring-greenhouse-gas-emissions

Solid Waste

The EPA's pre-built excel file to help measure and track your waste and recycling:
- http://www.epa.gov/smm/wastewise/measure-progress.htm

Greenbiz's comprehensive guide to reducing corporate waste:
- http://www.greenbiz.com/research/report/2004/03/09/business-guide-waste-reduction-and-recycling

Water Waste

BSR's guide on how to establish your water usage:
- http://www.bsr.org/reports/BSR_Water-Trends.pdf

EPA information about conserving water:
- http://water.epa.gov/polwaste/nps/chap3.cfm

Packaging

Links to get you started on sustainable packaging:
- http://www.epa.gov/oswer/international/factsheets/200610-packaging-directives.htm
- http://sustainablepackaging.org/uploads/Documents/Definition%20of%20Sustainable%20Packaging.pdf

Sustainability Practices

Ideas for alternative transportation programs:
- http://www.ctaa.org/webmodules/webarticles/articlefiles/SuccessStoriesEmpTranspPrograms.pdf

The EPA environmentally preferable purchasing guidelines for suppliers:
- http://www.epa.gov/epp/

EPA life cycle assessment information:
- http://www.epa.gov/nrmrl/std/lca/lca.html

Green Seal green products & services:
- http://www.greenseal.org/FindGreenSealProductsandServices.aspx?vid=ViewProductDetail&cid=16

Ecologo cleaning and janitorial products:
- http://www.ecologo.org/en/certifiedgreenproducts/category.asp?category_id=21

EPA information on sustainable landscape management:

- http://www.epa.gov/epawaste/conserve/tools/greenscapes/index.htm

ARIZONA STATE UNIVERSITY

Financial Services

FATCA Compliant Substitute W-9

RETURN TO ASU		DO NOT SEND TO IRS

ATTN: Foreign individuals who are non-residents for US tax purposes only complete IRS Form W-8BEN. Foreign entities complete IRS Form W-8BEN-E.

► Taxpayer Identification Number (TIN)		☐Employer ID Number (EIN) ☐Social Security Number (SSN)

► LEGAL NAME: (must match TIN)	
► LEGAL MAILING ADDRESS:	(Where tax information and general correspondence is to be sent)
DBA/Branch/Location:	
ADDRESS LINE 1:	
ADDRESS LINE 2:	

CITY:		ST:		ZIP:	

► REMIT TO ADDRESS:	☐ Same as Legal Mailing Address
DBA/Branch/Location:	
ADDRESS:	
ADDRESS LINE 2:	

CITY:		ST:		ZIP:	

► ENTITY TYPE (EP: exempt payee [backup withholding] exemption code; FC: FATCA exemption code)

☐Individual (not a business)	☐ Sole proprietor (individually owned business) or sole proprietor organized as LLC or PLLC	☐Corporation (not providing health care, medical or legal services) (EP: 5)	☐Corporation (providing health care, medical or legal services) (EP: 5)	☐Partnership, LLP or partnership organized as LLC or PLLC
☐The U.S. or any of its political subdivisions or instrumentalities (EP: 2 FC: B)	☐A state, a possession of the US or any of their political subdivisions or instrumentalities (EP: 3 FC: C)	☐Tax-exempt organizations under IRC §501 or §403 (EP: 1 FC: A)	☐An international organization or any of its agencies or instrumentalities (EP: 4)	☐State of Arizona employee

Corporations: Is your or an affiliated company's stock regularly traded on one or more established security markets?
☐Yes ☐No (FC: D/E)

► CERTIFICATION

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct TIN (or I am waiting for a number to be issued to me).
2. I am not subject to backup withholding because I am exempt from backup withholding, I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding.
3. I am a U.S. citizen or other U.S. person (defined below).
4. The FATCA codes entered on this form, if any, indicating that I am exempt from FATCA reporting are correct.

Certification instructions. You must cross out item 2 if you have been notified by the IRS that you are currently subject to backup withholding because you failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN.

Signature of U.S. Individual	Date:

NOTE: *IF BOTH PAGES OF THIS FORM ARE NOT COMPLETED THE FORM WILL BE RETURNED TO YOU.* **Arizona State University (ASU) is fulfilling a mandate associated with state agencies increasing procurements from Arizona Small and Diverse Businesses.**

ARIZONA STATE UNIVERSITY

Financial Services
Vendor Authorization Form

RETURN TO ASU		DO NOT SEND TO IRS

► **Legal Name:**	**TIN:**

Are you doing business in Arizona for purposes of sales/use tax collection and remittance? ☐ Yes ☐ No

If you select Yes, please provide your Arizona License # and sales/use tax rate charged % DUNS#

SECTION 1 - FEDERAL INFORMATION

What is your business' federal classification type? See the definitions in the link or on the Vendor Authorization Form instructions. (S.B.A. Small Business definition FAR 19.001 and size standards FAR 19.102) http://www.sba.gov/size

Large Business? YES ☐ NO ☐
Small Business? YES ☐ NO ☐

Please check all that apply to your business for the federal supplier type or check Not Applicable here: ☐

Service-Disabled Veteran-Owned (VD) ☐	Small Disadvantaged (SD) ☐	Women-Owned (WO) ☐
Veteran-Owned (VO) ☐	Minority Institution (MI) ☐	HUB Zone (HZ) ☐

SECTION 2 - STATE OF ARIZONA SMALL BUSINESS INFORMATION

Are you self-certified according to this State of Arizona definition? **"Less than 100 full-time employees OR less than $4 million in volume in the last fiscal year"**	YES ☐	NO ☐

Per FAR 52.219-1 and under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a small, HUB Zone small, small disadvantaged or women-owned small business concern to obtain a contract to be awarded under the preference programs established pursuant to section 8(a), 8(d), 9 or 15 of the Small Business Act or any other provision of federal law that specifically references section 8(d) for a definition of program eligibility, shall be punished by imposition of fine, imprisonment or both; be subject to administrative remedies, including suspension and debarment; and be ineligible for participation in programs conducted under the authority of the Act.

Print Name:	
Signature:	

Phone:	Fax:
Email:	

VENDOR: List the product or service provided.			
If the buyer name is listed, please **return** to the buyer.	Buyer:	Phone:	Email:

NOTE: *IF BOTH PAGES OF THIS FORM ARE NOT COMPLETED THE FORM WILL BE RETURNED TO YOU.* **Arizona State University (ASU) is fulfilling a mandate associated with state agencies increasing procurements from Arizona Small and Diverse Businesses.**

SECTION XIV – SECURITY REVIEW PROCESS (Reference Document #1)

Form version: 2016-06-20

Expectations

This checklist is to be filled out by the ASU project team, because the ASU project team is responsible for designing and implementing security controls. Vendor provided documents and diagrams are not sufficient.

Please have your answers completed and your **Security Architecture Diagram** available in your google project folder one week before your scheduled review. Projects with incomplete documentation will be asked to reschedule.

A preliminary review may be held, and is recommended, early in a project's lifecycle while there is still time to change course if design issues are identified. The final review should be held shortly before the project goes live, when the contemplated servers have been set up at least to the point where the required vulnerability scans can be done.

Overview

The ASU security review process is designed to guide each project team to implement solutions efficiently while minimizing security risks. At the beginning of a project, for most of the questions below the answer will probably be "Unknown". As design and development continues, you can start filling in the answers you know. When you are ready for a discussion with an Information Security Architect, please email Security.Review@asu.edu

Where you see the checkbox "☐" symbol below, if that is your answer, delete the checkbox and replace it with an "X".

Projects do not always achieve a "perfect" score; however the goal is to reduce all risks to low or addressed. The purpose of this document is to allow management to get an evaluation of the risk in this project as compared to other projects and ASU standards.

Scope of Review

It is not practical to bring all existing systems up to current standards. Instead, our goal is "No new bad". So for each project we look at what changes are being made as part of that project. This includes:

- New hardware
- New software developed for the project: web sites or otherwise
- New software acquired, installed here, hosted elsewhere...
- New software in the form of a "cloud service" or similar
- New connections between new or existing systems
- New data flows between new or existing systems
- New data stores: added tables or columns, data files, network shares...

For our purposes "new" means new to ASU -- it has not been through an ASU Security Review before. So if ASU starts using an existing "cloud service" that service should be reviewed even if the service is not implementing any changes for ASU's project.

Also if an existing system is changed for the project, the change is "new" because it hasn't previously been reviewed.

Example: Existing system "A" regularly transfers a data file to existing system "B". The project will add software that runs on "B" and makes a new use of the data on "B". System "B" is in scope because it is being changed, but system "A" and the data file transfer are not in scope because they are not changing. System "A" can still be shown on your Security Architecture Diagram to clarify the workflow.

Project Information

What is the name of your project? Please use the same name that appears in project status systems.

If you are using Planview for project management, what is the Planview project ID number (usually 4 to 7 digits?

X This project is not using Planview.

What is the purpose of your project? Briefly describe what you'd like to accomplish.

Who is the Steward for the project (the ASU employee who decided we should do this, the sponsor from a business perspective)?
Name:
Title:
Department:

Who is the Technical Administrator for this system (the ASU employee who will manage ongoing system maintenance, enhancement and patching or manage the vendor who will perform this function)?
Name:
Title:
Department:

(For separation of duties reasons, the Steward and the Technical Administrator should not be the same person. Technical people implement business requirements. Technical people should not unilaterally create systems for which there is no business requirement or sponsor.)

Responsibility for Secure Design

Security practitioners have found that to be effective, security measures must be "baked in from the beginning" rather than "pasted on at the end". This is one of the reasons for using a **System Development Life Cycle** (mentioned elsewhere in this checklist) that includes security checkpoints as the project progresses.

Attackers usually take advantage of mistakes. These flaws frequently arise at the boundaries between independent components, due to misunderstandings or weaknesses in how the parts are put together. This means you can have a collection of "secure" ***parts***, but yet not have a secure ***whole***. Someone must create a holistic design that ensures all the parts fit together in a way that complies with regulations and ASU standards.

Who is responsible for the secure design of the entire system?

☐	**Unknown**	We don't know who is responsible for the security design of the entire system.
☐	**High**	Although certain parts may be designed for security, nobody is responsible for the security design and ASU standards compliance of the entire system including users and their devices.
☐	**Medium**	A vendor claims to be responsible for the security design and ASU standards compliance of the entire system, but the vendor has not signed ISO language, or the scope of the vendor's contracted responsibility does not cover the entire system including users and their devices.
☐	**Low**	A single vendor has accepted responsibility for all of the security design and ASU standards compliance, has signed ISO language, and the scope of the vendor's contracted responsibility covers the entire system including users and their devices.
☐	**Addressed**	One or more ASU employees have designed the system with a holistic security perspective from the beginning, selecting components and/or vendors that meet regulatory requirements and ASU standards. The ASU employee(s) responsible for the security design and ASU standards compliance are: _____ _____

Additional information (optional)

Sensitive Data

The expectations for the project's security measures depend on how much harm could occur when things go wrong. For definitions of the following data classifications please see the Data Handling Standard at http://links.asu.edu/datahandlingstandard

What is the most sensitive data in this project? (Check all that apply.)

Regulated Data

☐ PCI regulated (credit card data)

☐ FERPA regulated (student data)

☐ HIPAA regulated (health data)

☐ ITAR (import, export, defense-related technical data or foreign students)

ASU Data Classifications

☐ Highly Sensitive - disclosure endangers human life health or safety

☐ Sensitive - regulated data (including regulations above) or Personally Identifiable Information

☐ Internal - a login is required

☐ Public - anyone can see it without logging in

Additional information (optional) - examples of sensitive data elements etc.

Note: If you checked *any* of the highlighted boxes above, ASU's Data Handling Standard calls for this data to be encrypted for all new systems, and an encryption transition plan for existing systems. In addition, encryption is recommended for all data classifications on all systems. If you can, encrypt everything everywhere.

One reason for encryption in transit is to prevent other computers on the network from reading sensitive data as it goes by.

How will sensitive data be protected in transit, as it travels across the network? (Check all that apply.)

☐	**Unknown**	We haven't determined this yet, for some or all connections.
☐	**High**	Sensitive data will be traveling across one or more connections without any protection.
☐	**High**	All systems and connections storing or processing sensitive data are within the ASU data center, but sensitive data is not encrypted as it moves from system to system.
☐	**High**	Firewalls, network segmentation, and/or other techniques limit sensitive traffic to only those systems that are intended to receive it. Other systems are prevented from connecting, or listening to sensitive traffic. However, sensitive data is not encrypted in transit.

☐	**Addressed**	All sensitive data is encrypted as it travels over each network connection.
☐	**Addressed**	All* web sites are using https encryption. Servers have valid https certificates. (The certificates are correctly configured and installed so that no warnings are seen.)
☐	**Addressed**	This project has no sensitive data.
☐	**Addressed**	This question is not applicable for this project because all of the following are true: ● No ASU equipment or network connections will be used to transmit sensitive data. ● If a vendor is transmitting or receiving sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language.

Additional information (optional)

* Note: ASU Information Security recommends https encryption for all web pages, whether there is sensitive data or not. Here are some reasons:

● Some Internet Service Providers have started altering page content so you don't see what you requested, you see what they want you to see. Thus even the simplest public static web page can be abused. The http protocol cannot detect this; https can.

● An increasing variety of entities are interested in eavesdropping on your Internet use, which also becomes much harder under https.

● Google gives preference to https pages in its search results: see http://googleonlinesecurity.blogspot.in/2014/08/https-as-ranking-signal_6.html

---

Encryption at rest is a defense against the possibility that media might be misplaced, stolen, or not disposed of properly. Sensitive data should be protected wherever it goes -- on servers, desktops, laptops, mobile devices, and backups of these systems.

How will sensitive data be protected at rest, wherever it is stored? (Check all that apply.)

☐	**Unknown**	We haven't determined this yet, for some or all devices.
☐	**High**	Sensitive data will be stored without any protection, on devices available to the general public without logging in.

☐	**High**	Sensitive data will be stored without encryption at rest, even though PCI or other applicable regulations require it.
☐	**Medium**	Sensitive data will be stored without encryption, but the devices require a login, and there is no applicable regulation requiring encryption at rest.
☐	**Medium**	All systems storing or processing sensitive data are within the ASU data center, but sensitive data is not encrypted on disk. There is no applicable regulation requiring encryption at rest.
☐	**Low**	Sensitive data is encrypted on disk, but not on backups. There is no applicable regulation requiring encryption at rest.
☐	**Addressed**	All sensitive data is encrypted at every location where it is stored, including user devices and backups.
☐	**Addressed**	This project has no sensitive data.
☐	**Addressed**	This question is not applicable for this project because all of the following are true: ● No ASU equipment will be used to store sensitive data. ● If a vendor is storing sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language.

Additional information (optional)

Security Architecture Diagram

For instructions on how to create a security architecture diagram, please see How to Create a Security Architecture Diagram. Note: not all diagrams are security architecture diagrams suitable as the roadmap for your review.

Include administrative interfaces. Although they may not be intended for users, they are still a potential point of attack and, given the privileged access they provide, are even more valuable to attackers.

A Security Architecture Worksheet (example here) is not required, but it can help you gather the information needed for your diagram. You may find a blank worksheet in your security review folder. If not, you can request one by email to security.review@asu.edu

Has a complete security architecture diagram been submitted?

☐	**Unknown**	The security architecture diagram has not yet been submitted.
☐	**Unknown**	There are one or more diagrams, but they are incomplete, inconsistent, or do not provide the necessary information (all endpoints with fully qualified DNS hostname or IP address, all connections with protocol, encryption type, and listening port). The rating is "Unknown" because there may be systems or connections that are not reviewed because they are not detailed on the diagram.
☐	**Unknown**	A diagram has been submitted, but it is a vendor's generic diagram and does not show ASU specific systems, hostnames, IP addresses, connections, or other details. The rating is "Unknown" because there may be systems or connections that are not reviewed because they are not detailed on the diagram.
☐	**Addressed**	The security architecture diagram includes every endpoint that will be part of the project, and every connection between endpoints. Every endpoint that listens for connections is identified with its fully qualified DNS hostname and/or IP address. Every connection is labeled with protocol, encryption type if any, and port number on the listening device.
☐	**Addressed**	The security architecture diagram includes every ASU specific endpoint and connection, but not vendor internal architecture. However all connections from ASU to the vendor's border are shown, and the vendor has signed a contract including ISO language accepting responsibility for adequately protecting ASU's sensitive data. Every ASU endpoint that listens for connections is identified with its fully qualified DNS hostname and/or IP address. Every ASU connection is labeled with protocol, encryption type if any, and port number on the listening device.

If you checked one of the answers saying there is a diagram, please upload a copy of it to your google Security Review folder and fill in its document name here:

Additional information (optional)

☐ Has this project been to the Architecture Review Board? (Suggestion: share this document with ARB to provide advance answers to many possible ARB questions.)

Servers

As you look at your Security Architecture Diagram you will most likely see two types of endpoints: clients and servers. A server is any device that listens on a defined port for incoming connections.

Each server used by your project should be shown on the diagram (unless all connections to the server occur inside a vendor's "cloud", the vendor has signed ISO language, and ASU cannot make any changes to the server's software or configuration). If the server is new for your project, or is being changed for your project, the server should be scanned for vulnerabilities that may be introduced by your changes.

List each server's fully qualified DNS hostnames and/or IP addresses here:

(Note: A DNS name is not a URL. URLs for web servers are requested in a different question.)

If you filled out a Security Architecture Worksheet (example here) you probably already have some of this information on the first tab (endpoints) under the Servers heading.

Production (intended for normal use)

QA (should be virtually identical to production)

Development (for unfinished work, programmer testing etc.)

Additional information (optional)

Have the above servers been scanned or penetration tested for security vulnerabilities? What was the outcome? Note: to request a server scan send email to scanrequest@asu.edu

☐	**Unknown**	Some new or changed servers have not yet been scanned or penetration tested.

☐	**High**	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
☐	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
☐	**Low**	A vendor says the server(s) have been scanned or penetration tested and issues have been addressed but we do not have evidence (e.g. a copy of the report).
☐	**Addressed**	All new servers have been scanned or penetration tested. No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix. We have evidence of the scan (e.g. a copy of the report).
☐	**Addressed**	This project has no new servers and no changes to existing servers (other than servers inside a vendor's "cloud" and the vendor has signed ISO language).

Additional information (optional)

Web Servers

Each device that accepts connections using the http (or https) protocol is a web server. In addition to the server vulnerability scan above, each web site on a web server should be scanned.

A "web site" is anything that responds to the Hypertext Transfer Protocol (HTTP) whether or not a traditional web browser is used. The term includes, for example, Web Services and device control interfaces, in addition to human-oriented "web applications".

To facilitate automated vulnerability discovery (scanning) a web site should have an entry point that provides links, directly or indirectly through intermediate pages, to all of the URLs offered by that site. For example, some web services use a WSDL to allow automated enumeration of the available calls and parameters. Any URLs that are not found by automated testing should be manually tested for potential security vulnerabilities.
The web site may offer more than one entry point, for example to support different user roles. In this case each entry point should be listed. If you filled out a Security Architecture Worksheet (example here) you probably already have some of this information on the third tab (web sites).

If your project includes new web sites or changes to existing web sites show their entry point URLs here:

Production (intended for normal use)

QA (should be virtually identical to production)

Development (for unfinished work, programmer testing etc.)

Additional information (optional)

Based on the above URLs, do the web sites have adequate test environments?

☐	**Unknown**	At present we don't know if there will be development or QA instances of the web site(s).
☐	**Medium**	Only a production instance exists. There is no place to test code or changes without impacting live systems and data.
☐	**Low**	A QA or development instance exists, but it is different from production to the extent that there could be flaws in one environment that do not exist in the other.
☐	**Addressed**	All sites have QA instances that are sufficiently identical to production that the results of tests in QA can be relied on to evaluate the production instance.
☐	**Addressed**	This project has no web sites.

Additional information (optional)

Have these new web sites or changes to existing web sites been scanned or penetration tested for security vulnerabilities? What was the outcome? Note: For best results, we recommend scanning QA first, then after any issues are resolved and migrated to production, scan production to verify the fixes. To request a web scan send email to scanrequest@asu.edu.

☐	**Unknown**	Some web sites have not yet been scanned or penetration tested.
☐	**High**	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
☐	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
☐	**Low**	A vendor says the site has been scanned or penetration tested and issues have been addressed but we do not have evidence (e.g. a copy of the report).
☐	**Low**	All sites have been scanned or penetration tested, but the tests were not run against the production site or against a QA site that is essentially identical to production. No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix.
☐	**Addressed**	All sites have been scanned or penetration tested against the latest version of code that has gone live or will go live. Tests were run against the production site or against a QA site that is essentially identical to what is or will be in production. Either ASU did the scan, or we have evidence of the scan (e.g. a copy of the report). No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix.
☐	**Addressed**	This project has no web sites.

Additional information (optional)

Based on the project's access to sensitive data, what is the proposed criticality rating of your web site(s)?

For a definition of "criticality" see the Web Application Security Standard at http://infosec2.uto.asu.edu/files/web%20application%20security%20standard.pdf.

☐High	The web site will have access to modify the authoritative source of sensitive data. (To request that an application be considered for ASU's High Criticality list, submit a request to your Security Review Architect.)
☐Medium	The web site has access to sensitive data, but is not rated High.
☐Medium-Low	The web site has confidential data, but not sensitive data. (Most web sites with a password fall in this category, unless they have sensitive data, which would be Medium or High.)
☐Low	The web site only has public information. Web sites in this category do not use a password.

Additional information (optional)

Database Servers

Servers that have databases containing sensitive data should be protected from various types of attacks. A database server directly connected to the Internet has no defenses except the ID and password that may be required. A database server directly connected to a web server may lose *even that ID/password defense* if the web server is compromised.

What database protections are in place?

☐	**Unknown**	The database protections have not yet been determined.
☐	**High**	There are one or more databases with access to sensitive data. The database servers have publicly routable IP addresses and there is no firewall limiting connections to the database. People from anywhere in the world can connect directly to the database server.
☐	**Medium**	A database containing sensitive data is directly accessible by a web server, but the database only accepts requests from the web server. Other devices cannot make connections to the database.
☐	**Low**	Web servers can connect to database servers directly, but alternate protections are in place to defend the database from a web server compromise, such as a Web Application Firewall in front of the web server. (Describe in the notes how the protective technology protects the database from a web server compromise.)

☐	**Addressed**	Web servers cannot connect directly to database servers due to network segmentation, firewall rules, etc. Web servers interact with database servers through an application server that only permits a white list of known good transactions (a three tier architecture). Web servers also have defenses against typical attacks (such as SQL injection) via parameterized queries, stored procedures, or other techniques that do not pass arbitrary strings to the SQL command interpreter.
☐	**Addressed**	None of the systems in this project have access to a database containing sensitive data.
☐	**Addressed**	This question is not applicable for this project because all of the following are true: ● No ASU equipment will be used to store a database with sensitive data. ● If a vendor has a database with sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language.

Additional information (optional)

User Authentication

How do the project's systems verify user identity and access rights?

☐	**Unknown**	User authentication systems have not yet been defined.
☐	**High**	When a user logs in, their password is sent across the network without encryption. For example, users log in from a web page that does not use https encryption. Or as another example, users have client software on their computers which logs in to a server, but the connection to the server is not encrypted.
☐	**High**	One or more systems maintain an independent user authentication technique instead of standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
☐	**Medium**	The login page uses https encryption and standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS, but subsequent pages revert back to http.
☐	**Low**	Ordinary users are authenticated using standard ASU enterprise "single-sign-on" systems, but privileged users, such as site owners or administrators, are authenticated using a separate mechanism.

☐	**Addressed**	All systems that require users to identify themselves use standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
☐	**Addressed**	Because all data is public, no user authentication is needed. Administrator access is controlled through existing mechanisms outside the scope of this project.

Additional information (optional)

Servers Authentication

When one server connects to another server, both ends of the connection should have a way to verify that the other server is the correct one and not an impostor.

How do the project's servers authenticate each other?

☐	**Unknown**	Server authentication techniques have not yet been defined.
☐	**High**	One or more servers initiate or accept connections with their peers, but do not verify or otherwise restrict which servers can connect.
☐	**High**	When a server logs in to another server, a password or other secret is transmitted across a network connection without encryption.
☐	**Medium**	Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a "black list" identifying which addresses are not allowed to connect.
☐	**Low**	Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a "white list" specifically identifying which addresses are allowed to connect, and denying all others by default.
☐	**Low**	Servers use credentials to identify each other, but there are weaknesses (explain in the notes). For example: (A) the credentials are not unique to one application (B) the credentials are not safely stored, or (C) it is difficult to change the credentials.

☐	**Addressed**	Each server uses a standard mechanism, such as https, to verify the other server's identity when initiating a connection to another server. If using https, servers have valid https certificates, and clients verify certificate validity. (The certificates are correctly configured and installed so that no warnings are seen.) The listening server authenticates the requesting server using credentials that are unique to this application. The credentials are not stored where they can be accessed without authorization. Credentials are periodically updated, and can be quickly updated if a compromise is suspected.
☐	**Addressed**	The project does not have more than one server, so there is no need for servers to authenticate each other.
☐	**Addressed**	The changes being made as part of this project will not affect a situation where two or more servers are communicating with each other, so the question does not apply.

Additional information (optional)

Vendor Involvement

☐ This project is being done entirely by ASU employees, including development and hosting of all components.

If you did not check the box above, list the companies or people contributing to this project who are not ASU employees, and indicate when (if) the vendor agreed to ISO Contract Language**:**

Any vendor that provides hosting services, physical or virtual, has access to the data stored or processed there. Thus even hosting providers should be included in your list of vendors.

Vendor	**Date vendor signed contract with ISO language**

Additional information (optional)

Is there a contract with each vendor, and does the contract include ISO language?
Note: ISO's standard contract language can be found here and is essential for contracts involving sensitive or highly sensitive data.

☐	**Unknown**	Vendors have not yet been selected, or the decision to do this entirely within ASU has not been finalized.
☐	**Unknown**	Status of vendor contract(s) or inclusion of ISO language is presently unknown.
☐	**High**	There are one or more vendors with whom we do not yet have a contract.
☐	**Medium**	There is a contract with each vendor, but one or more contracts do not include current ISO language. The vendor is not willing to change the contract to include ISO language.
☐	**Low**	There is a contract with each vendor, but one or more contracts do not include current ISO language. The vendor is willing to change the contract to include current ISO language.
☐	**Addressed**	There is a contract with each vendor, and each contract includes current ISO language.
☐	**Addressed**	This project has no vendor involvement.

Additional information (optional)

Backup, Disaster Recovery, and Business Continuity Strategy

Systems should be able to recover from damaging events such as hardware failures or accidental or malicious data or software corruption.

What is the backup strategy?

☐	**Unknown**	The backup strategy has not yet been determined.
☐	**High**	There are no backups of some or all systems that are relied upon to store data.
☐	**Medium**	Backups are being made, but the ability to fully restore after a total data loss has not been tested.
☐	**Low**	All essential systems are regularly backed up. Restore capability is tested at least once a year. If data or software damage or loss were to occur, restoring the latest backup or reinstalling the software would be sufficient; the loss of updates since the last backup would be tolerable.
☐	**Addressed**	All essential systems are frequently and automatically backed up to a separate physical location. Restore capability is tested at least once a year. Audit logs or other mechanisms are in place that can back out accidental or malicious changes.
☐	**Addressed**	Not applicable. The systems involved in this project are not the authoritative store of any data. It could be recreated from elsewhere if lost, so no backups are needed. Original software install media and ASU-specific install instructions will be kept in a safe place so that the system can be rebuilt in the event of hardware failure or system corruption.

Additional information (optional)

For the following question, your project has "Mission Critical" components if any of the following are true:

- Any web site associated with this project has a "Tier 1" rating. (The Web Application Security Standard at https://getprotected.asu.edu/sites/default/files/web%20application%20security%20standard.pdf defines these ratings.)
- There are regulatory requirements that mandate Disaster Recovery and/or Business Continuity planning.
- Your project sponsor wants this considered a "Mission Critical" system for some other reason (by whatever definition is meaningful to the sponsor).

A plan is recommended whether your project includes Mission Critical elements or not. However, expectations are higher for Mission Critical components.

☐ This project has no Mission Critical components.

Have you documented and tested your disaster recovery and business continuity plan?

☐	**Unknown**	We do not currently know the status of Disaster Recovery and Business Continuity plans.
☐	**High**	This is a Mission Critical project but it doesn't currently have Disaster Recovery and Business Continuity plans.
☐	**Medium**	Disaster Recovery and Business Continuity plans don't exist at this time, however, the project is not Mission Critical.
☐	**Medium**	The Disaster Recovery and/or Business Continuity plans have been drafted, but key elements are missing, for example: redundant systems are not in place, contracts with vendors are not finalized, or the plan has not been tested.
☐	**Low**	All mission critical components have geographically-dispersed redundancy with enough capacity to sustain mission critical operations during an extended loss of the primary systems. Disaster Recovery and Business Continuity plans are in place, complete with any contracts for vendor services during an adverse event. However, these are not regularly tested by staging mock disaster scenarios.
☐	**Addressed**	All mission critical components have geographically-dispersed redundancy with enough capacity to sustain mission critical operations during an extended loss of the primary systems. Disaster Recovery and Business Continuity plans are in place, complete with any contracts for vendor services during an adverse event. Systems, plans, and recovery-critical personnel are tested annually by staging mock disaster scenarios.
☐	**Addressed**	The Disaster Recovery and/or Business Continuity plan has been documented and tested, and there are no Mission Critical components. (Projects with Mission Critical components should choose one of the other answers.)

Additional information (optional)

If this project is "Mission Critical", please upload a copy of your plans to your google Security Review folder and fill in the document name(s) here:

Logging and Alerting

Please see ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard for information about what is required to be logged.

Systems should be designed to recognize and alert on typical attacks. For example, authentication or authorization systems should watch for brute force password attempts or other unauthorized access. Web servers, or protective appliances, should watch for the OWASP Top Ten Vulnerabilities and similar attacks.

Do systems watch for undesirable or unexpected activity and log these events? Do logged events trigger alerts? What happens then?

☐	**Unknown**	The availability of logging is presently not known.
☐	**High**	Some systems do not recognize and log typical attacks, or other unexpected or undesired events.
☐	**Medium**	Potential security events are logged, but there is no human or automated review of those logs to alert on possible problems.
☐	**Medium**	Potential security events are logged, but the logs do not fully comply with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard.
☐	**Low**	Logs are maintained in compliance with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard, alerts are raised when appropriate, but staff may not be available to respond to the alerts.
☐	**Addressed**	Logs are maintained in compliance with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard, events are raised when appropriate, and staff will be available to respond to the alerts throughout the lifecycle of the application.

Additional information (optional)

Software Integrity

Whoever writes your software gains control of your computer, sensitive data, and identity. Thus it is important to be sure the software comes from sources you trust. Verify the origin of software before installing it, and keep it up to date if security fixes have been released.

Current versions should be originally installed, upgrades should be applied when available, and security patches should be applied promptly. During original installation or subsequent updates, controls should be in place to ensure that all software comes from trustworthy authors, and has not been tampered with along the way.

Are current versions of software being deployed? Will upgrades and patches be promptly applied?

☐	**Unknown**	Version and/or patch management information is presently unknown for one or more systems.
☐	**High**	Some systems run outdated versions of their operating system, utilities, or installed applications. Or, systems are initially deployed with current software, but nothing will be in place to keep them current in the future.
☐	**Medium**	There is a capability in place to distribute the most recent software version or updates, but it does not have controls to protect against fake (malicious) updates.
☐	**Low**	Initial install files and/or updates carry a signature (e.g. a hash or checksum) to verify file integrity, but the file must be (and will be) manually checked against a trusted list of valid signatures.
☐	**Addressed**	Software, including operating system, utilities, applications, and any other executable code, is only obtained from trusted sources. It is distributed using mechanisms that automatically ensure it is not altered, for example, files are cryptographically signed or delivered over a channel that ensures end-to-end file integrity. Current versions of software are initially installed. Patching and upgrades are performed regularly and as needed. Patches are automatically verified so that administrators and users cannot be tricked into installing a malicious update.
☐	**Addressed**	This project does not include any new software. Nothing new is installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

Additional information (optional)

ASU's Software Development Life Cycle (SDLC) standard (https://getprotected.asu.edu/sites/default/files/Software_Development_Life_Cycle.pdf) calls for all software development

to occur within an SDLC that includes information security controls and separation of duties to help ensure the controls are effective.

Is the software included in this project developed under a written Software Development Life Cycle?

☐	**Unknown**	We do not know if software (including vendor software, ASU developed software, or software obtained from other sources such as libraries or frameworks) is or was developed under the control of a written SDLC.
☐	**High**	One or more software components used within this project have no SDLC.
☐	**Medium**	An SDLC exists, but it is not written, it is not routinely followed, or it does not include security controls.
☐	**Low**	We have evidence that a written SDLC with security controls is routinely followed, however the development organization does not have enough people to implement full separation of duties.
☐	**Addressed**	All software (including vendor software, ASU developed software, and software libraries imported from other sources) is or was developed under the control of a written SDLC which includes security checkpoints and separation of duties to control the advancement of software past those checkpoints.
☐	**Addressed**	This project does not include any new software. Nothing new has to be installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

If you checked one of the answers saying there is a written SDLC, please upload a copy of it to your google Security Review folder and fill in its document name here:

Additional information (optional)

Has the new software developed or purchased in this project undergone vulnerability scanning or penetration testing by an entity other than the developer?

☐	**Unknown**	The status of vulnerability scanning or penetration testing is not known at this time.

☐	**High**	One or more components of new software (other than web sites) have not been vulnerability scanned or penetration tested.
☐	**Medium**	Vulnerability scanning or penetration testing has been performed, but by a member or close affiliate of the development team or vendor, such that its independence is not assured.
☐	**Low**	New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, however some issues remain unaddressed. The project team has evaluated the open issues and does not consider them a risk to ASU (explain in notes below).
☐	**Addressed**	New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, and any issues found have been addressed.
☐	**Addressed**	Vulnerability scanning or penetration testing is not required for this project because there is no new software other than web sites, and the web sites have been scanned for security vulnerabilities.
☐	**Addressed**	This project does not include any new software. Nothing new has to be installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

Additional information (optional)

Deprecated or Dangerous Technologies

Frequently an exciting new technical capability is rapidly adopted without due consideration for the security consequences. Hackers begin taking advantage of weaknesses, so some technologies carry added risk. Users can defend themselves by

disallowing unwanted technologies, but then some web sites refuse to serve those users until they place themselves at risk again.

Many of these techniques include automatically or manually downloading software from unknown or untrusted authors. Also see the **Software Integrity** section for additional questions that pertain to any executable code that is downloaded or installed such as a plug-in or media player.

Does the project require any of the following technologies in order to make full use of the system?

☐	**Unknown**	We do not know if the project will use any of the technologies listed in this section.
☐	**Medium**	Users are required to enable Java in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Java has become one of the top malware distribution mechanisms.)
☐	**Medium**	Users are required to permit Active-X controls. (Active-X controls give a web site more control of a user's computer, making it easier for attackers to exploit defects in the operating system, browser, or Active-X control itself. Also, dependence on Active-X locks out users of operating systems and browsers that may be more secure.)
☐	**Medium**	A password protected web site imports JavaScript code or other client-executed code from another web site that is beyond ASU's control. (This makes it possible for the other site's script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.
☐	**Medium**	A password protected web site imports JavaScript code or other client-executed code over an http (unencrypted) connection. (This makes it possible for a man-in-the-middle to inject a script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.
☐	**Low**	Users are required to enable Flash in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Flash has become a common malware distribution mechanism.)
☐	**Low**	Users are required to allow pop-up windows in their browsers. (Several popular web browsers now disable pop-ups by default because they have been abused by advertisers and malware.)
☐	**Low**	The web site only allows certain browsers, and refuses service to users of other browsers. (Such web sites frequently lock out users of operating systems and browsers that may be more secure.)
☐	**Low**	Users are required to enable or install other plug-ins or media players not listed above. (Please describe in notes below.)
☐	**Addressed**	The project uses one or more of the above technologies, but they are entirely optional. Users can still accomplish all the functions of the system even if the user shuts off the deprecated technologies.

☐	**Addressed**	The project will not use any of the technologies listed in this section.

Additional information (optional)

Other Risks

If you are aware of other risks you would like to document, describe them here and assign what you think is the appropriate risk rating, considering the classification of the data involved. (Copy and paste a table cell containing the rating you want to apply.)

☐		
☐		
☐		

Additional information (optional)

Risk Score

Total up the boxes checked above. Each question should have at least one box checked.

Risk Rating	**Unknown**	**High**	**Medium**	**Low**	**Addressed**
Count of boxes checked					

Approval

Please be aware that if your Risk Score includes any **Red** items, approval of the ASU Provost or CFO may be needed. **Orange** items may require approval of the sponsoring business unit's Dean or comparable leadership.

SECTION XIV- continued (Reference Document #2)

Upon award, the successful Proposer(s) is expected to submit a Security Architecture Diagram.

How to Create a Security Architecture Diagram
Revised 2016-05-27

This describes how to make a Security Architecture Diagram for a security review.

Here is the information you will need to gather to create a Security Architecture Diagram:

- Identify each role your new system will support. A role is a group of users who can all do pretty much the same things. For example your system may offer one collection of services to *students* and other services to *faculty*. These are two roles. Roles may also depend on the type of device being used. For example if mobile devices use an "app" instead of using the web site provided for desktop users, you probably have a *mobile users* role and a *desktop users* role, although different descriptions may be more applicable.
    - Don't leave out the administrators. The *administrator* role is an important part of system maintenance, and privileged roles are an attractive hacker target.
- Identify each endpoint in the system. Each role will be an endpoint, and each type of server is also an endpoint. Endpoints include any device that sends or receives data. But if there are multiple devices that perform the same operation, they can be represented as a single endpoint. For example, we don’t need to distinguish each end user computer when they all do the same thing. Similarly, if there is a cluster of identical servers doing the same thing, that’s one endpoint.
- Identify each connection between endpoints. If data is moving, there must be a connection to carry it. But unlike a data flow diagram, what matters here is not *which way* the data flows (it might be both ways) but *which endpoint* initiates the connection. Usually a connection is requested by a client (for example, your web browser) and accepted by a server (the web site). The server is listening for connections, usually on a predefined port.
- If you make backups, that is yet another data flow from one endpoint to another. How does the data get there? Show the connection if it is network based, or describe the physical security if sensitive data is moved by hand (e.g. backup tapes to a vault).
- For each server, determine what IP address and/or Fully Qualified DNS hostname will be used by the server, and on what port(s) it will be listening. What protocol is being used to communicate over each connection? Is the data protected in transit? How do the endpoints of the connection authenticate each other? (How do they verify that they have connected to the correct endpoint?)

You are now ready to start making your drawing.

- Choose a symbol to represent the endpoints. Typically this is a box, but it could be something else. Draw a box (if that’s your choice) for each endpoint. Again, that would be one box to represent all the users who share a single role, and another box for each server (or group of identical servers). If different users connect to different servers, that would be a distinct endpoint. Don’t forget the users! The system can’t work without them.
- Label endpoints that are permanent (e.g. servers) with their IP address and/or Fully Qualified DNS hostname*. Users, of course, come and go all the time, and their IP address or name doesn’t matter.

- Choose a symbol to represent the connections. Typically this is a line, but it could be something else. Draw a line (or whatever) from each endpoint to each other endpoint with which it communicates.
- Choose a symbol to identify which end of the connection is the client and which end is the server. Remember that the server is passively listening on a port for requests, and the client is initiating those requests. You could represent this, for example, by an arrowhead on the server end of the line, indicating that the client sends a connection request to the server.
- Near the server end of the connection, identify the port number on which the server is listening.
- Indicate the communication protocol used by the connection. For example, a web site may use the http or https protocol. Even for public sites, https is preferred.
- Describe, on the diagram or elsewhere, what type of data is flowing along each connection. Is it confidential? Regulated? If the data is sensitive, describe how it is protected in transit. For example, is it encrypted? Using what type of encryption? Describe any controls to limit who or what can connect and fetch the information.
- If there is confidential or sensitive data, describe how it is protected at each endpoint of the connection. Is it encrypted at rest? If so, how? Is the endpoint protected by a firewall? If so, what does the firewall block or allow? Is the data viewed but not stored (e.g. by a client) so that secure storage is a non-issue?

*See https://en.wikipedia.org/wiki/Fully_qualified_domain_name

Summary

So for each server (anything that accepts connections) you should have:
- Fully Qualified DNS name and/or IP address
- Description of what it is or what it does (web server? database?)

For each connection you should have:
- Port number where the server is listening
- Protocol (http, ssh...)
- Sensitivity of data flowing across that connection
- Protection of data flowing across that connection, if it is not public (encryption? what type?)
- If the server authenticates the client, how? (User ID and password?)
- If the client authenticates the server, how? (For example https uses a server certificate signed by a known certificate authority, which the client can verify.)

Additional Info

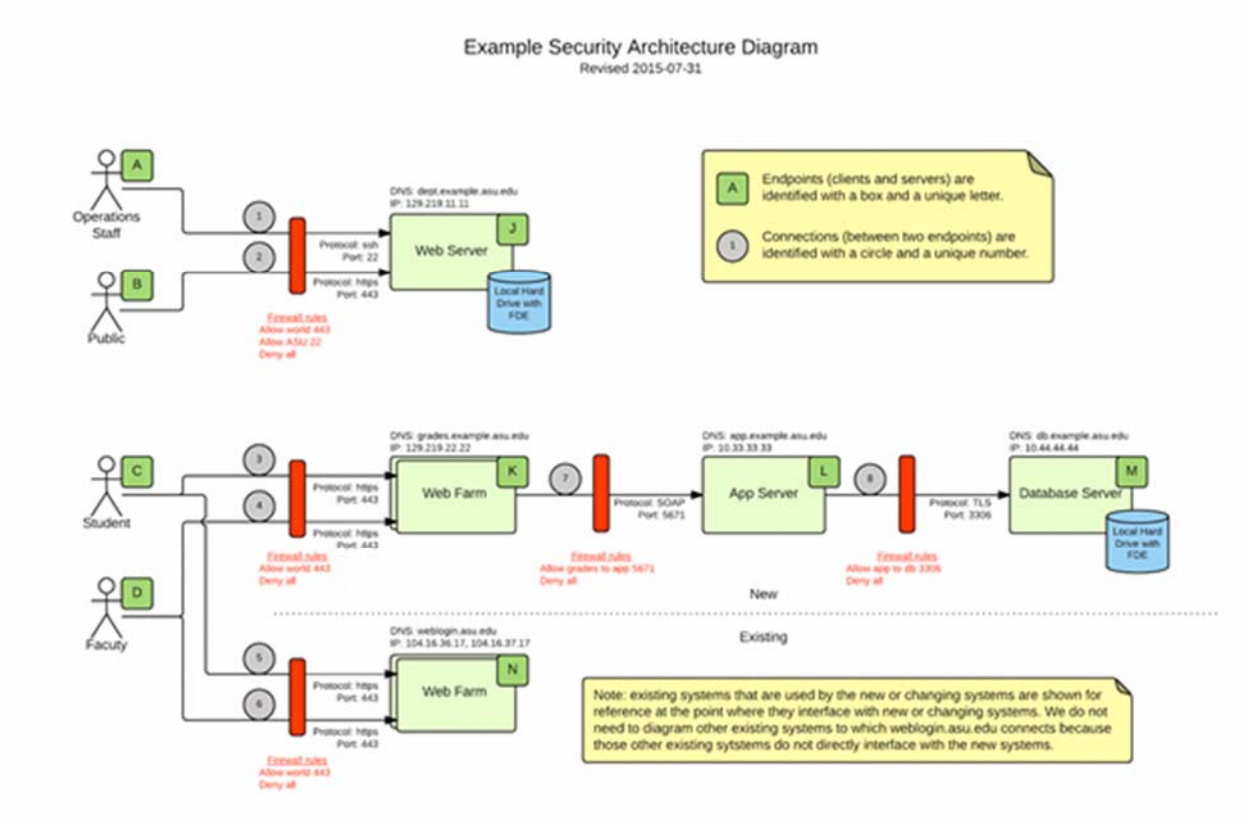
It may also help to distinguish existing endpoints, to which you will merely connect, from new endpoints that will be created as part of your project.

It may also help, if it is not obvious, to briefly describe the role or purpose of certain endpoints. For example: web server, database server, normal user, administrative user -- don't forget to show them too if they use different connections! Use consistent and unique names throughout; don't call it the "data server" here and "MySQL server" somewhere else and "repository" a third place.

It is not necessary to show disk drives that are physically within a single server. However network shares are most likely part of a file server, and the file server should also be shown as a distinct endpoint.

When you are done, save your diagram in a format that will open on other types of computers (e.g. pdf) for people who may not have your software.

EXAMPLES



The diagram need not be colorful. Although this diagram (below) is very simple, it conveys all the requested information. Visual appeal can be beneficial, but the factual information is what really matters.