April 30, 2019

REQUEST FOR PROPOSAL

Electronic Door Access, Video Surveillance, and Alarm Systems

RFP 221901

DUE: 3:00 P.M., MST, 05/28/19

Deadline for Inquiries	3:00 P.M., MST, 05/18/19
Time and Date Set for Closing	3:00 P.M., MST, 05/28/19

TABLE OF CONTENTS

SECTION I – REQUEST FOR PROPOSAL

RFP 221901

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Electronic Door Access, Video Surveillance, and Alarm Systems.**

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 Boulevard and Broadway Road) Tempe, Arizona 85281 **on or before 3:00 P.M., MST, 05/28/19. No proposal will be accepted after this time. 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 set for closing, will be returned to the proposer unopened.**

A representative of Purchasing and Business Services will announce publicly the names of those firms or individuals submitting proposals**.** 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

_____
Kevin Hall, Senior Buyer

KH/as

SECTION II – PURPOSE OF THE RFP

1. INTENT

ASU is seeking a qualified supplier(s) to provide services that may include but not be limited to the following: installation, support, training, upgrades, maintenance, and warranty of the ASU electronic door, video surveillance, and alarm systems. The management of these systems reside within the department of Preparedness and Security Initiatives (PSI), and is present on all ASU campuses. The purpose of the RFP is to find a suitable supplier(s) that can support all elements of the Integrated System for ASU Access Control (ISAAC) system:

a) Card access currently utilizing the Lenel OnGuard Pro System;
b) Video management supported by the GENETEC Video Management System;
c) Intrusion/panic alarms supported by Bosch hardware

Applying suppliers must be factory certified in the areas they support. The University may enter into a single contract with one supplier for all three (3) areas or issue multiple awards, whichever is in the University's best interest.

2. BACKGROUND INFORMATION

ASU's full security system uses HID iCLASS 16k smart chip technology. Currently, there are 5500+ readers, 1900+ cameras and many security/intrusion devices managed by the Preparedness and Security Initiative department and commonly known as "ISAAC".

ASU has two official ID cards known as the Sun Card and the Pitchfork ID Card. All ASU students, faculty, staff and partner affiliates may obtain an ASU ID card for use in the ISAAC system. All ASU credentials use the HID iCLASS 16k smart chip card.

Arizona State University is a new model for American higher education with an unprecedented combination of academic excellence, entrepreneurial energy and broad access. This New American University is a single, unified institution comprised of 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 100,000 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 two (2) year(s) with the possibility of three (3) 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

No pre-proposal conference will be held.

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 Boulevard 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 twenty (120) days** after the opening date and the right to accept a proposal not withdrawn before the scheduled proposal opening date.

13. **EXCEPTIONS:** The Arizona State University contract terms and conditions are included in this Request for Proposal in Section XII. These terms and conditions will 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 nonresponsive and may be rejected.** All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal. In no event is a Proposer to submit its own standard contract terms and conditions as a response to this RFP.

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, to:

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

Tel: 480-965-4370
E-mail: kevin.hall@asu.edu

All inquiries must be emailed to Kevin.Hall@asu.edu. 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,

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.

29. Other Opportunities with the University **NOT** related to this Request for Proposal.

The ASU Magazine

Connect your business with an affluent, educated audience through a business partnership with the ASU Alumni Association. The Association is the touchstone for the University’s 450,000 alumni and provides valuable connections between them and a wide variety of businesses. By doing business with the University, the largest university in the United States, your company can stand above the competition.

ASU alumni represent a responsive target market for your product or service.

- Alumni live worldwide.
- 230,000 of alumni reside in Arizona.
- More than 200,000 alumni live in Maricopa County.
- 38,000 of alumni reside in California.
- 55% of ASU alumni are under the age of 55.
- 85% own their own place of residence.
- 60% earn more than $50,000 annually.
- 40% fall in the top two highest wealth rating categories.
- 14% hold multiple and /or advanced degrees.

Specific partnership opportunities exist in a variety of areas.

- Advertise in the ASU Magazine, mailed to more than 400,000 homes around the world three times per year.
- Sponsor one of the Association's many programs and events and receive recognition and access to targeted audiences. Events include: Founder's Day, Homecoming, Legends Luncheon, Sun Devil 100, football tailgates, Career Fairs and many more! Create a unique partnership with us to suit your needs.
- Establish benefits for ASU alumni by offering targeted discounts and services to Sun Devil alums all over the world.
- Advertise on the ASU Alumni Web site or on our 110 Chapter/Club websites or in monthly E newsletter which is sent out to more than 240,000 people monthly. Cost is $1000 per month per each advertising venue.
- Learn more by Contacting John Davis at 480-965-5051 or jadavis@asu.edu today to start doing business with Sun Devil nation!

Sun Devil Sports Marketing

Sun Devil Sports Properties is the exclusive marketing and corporate sponsorship partner for Arizona State University Athletics and manages all corporate marketing opportunities surrounding Sun Devil Athletics. Sponsorship opportunities include, but are not limited to, on-premise signage, radio, print, digital, premium hospitality, event marketing and promotions. If you are interested in partnering with ASU Athletics, please contact Ben Burke at 480-727-9390.

Arizona PBS Delivers…

Arizona PBS, delivers award-winning, educational, cultural and current events programming to approximately 1.5 million viewers each week. Become an AZPBS sponsor.

- **AZPBS delivers – reach.** Comparable to other TV channels, well beyond cable channels and way beyond the top local radio stations and print media. AZPBS / KAET reaches 85 percent of the people of Arizona.
- **AZPBS delivers – quality audience.** Business leaders, decision makers, high income households, educated citizens & boomers and spenders with disposable income.
- **AZPBS delivers – marketing benefits:**
    - Build brand awareness by linking your business with high-quality programs
    - Generate community goodwill through support of public television
    - Promote your offerings to a broad audience at an affordable price
    - Market your brand in an environment free of commercial clutter
- **AZPBS delivers – multiple media platforms:**
    - 3 TV Channels – Eight HD, Eight Life & Eight World
    - Web views – www.azpbs.org (150,000 unique visitors a month)
    - E-Marketing – 40,000 email addresses … and more.

Contact: Chad Bowen at AZPBS corporate support at 602-496-8669 or Chad.Bowen@asu.edu
Kelly McCullough, General Manager at 602-496-2422 or Kelly.McCullough@asu.edu

SECTION V – SPECIFICATIONS/SCOPE OF WORK

1. SERVICES:

Proposers shall submit in one or multiple areas of physical security in support of ASU's ISAAC System. Proposers shall describe how your firm will meet the Specifications/Scope of Work Requirements below.

- Lenel OnGuard Pro system
- GENETEC Video Management system
- Bosch Intrusion hardware

2. QUOTES AND DESIGN SERVICES

Proposer will provide a specific and customized System Design Document (SDD), including a document typical for installations, hardware and software configuration specifications, network configurations, application and database specifications, and custom integrations, scripts, added fields or other system components to accommodate an all-encompassing architectural and software design for the ISAAC System.

Proposer will provide design services, including any engineering services, drawings, technical specifications, communications specifications, and other needed systems component designs to accommodate any facilities for the ISAAC System.

Proposer will work with PSI Representative to fulfill the necessary design services and provide the PSI Representative sufficient and certified expertise during all PSI Representative implementations, including software and hardware in new construction, remodels, and new adds for ISAAC services. All quotes developed for the PSI Representative will be accompanied by the following at a minimum and/or with an As Build:

a. Floor Plan with equipment marked
b. Legends for equipment markings
c. Proposed pathway for cabling
d. Estimated cable length per pathway
e. Equipment specification cut sheets
f. Detailed description of the Scope of Work
g. Roles and responsibilities per each item in the Scope of Work
h. Quotes with over 60 total readers will require a Lenel Reader Upgrade to be included in the quote.

Proposer will be expected to work with several PSI Representative departments and third-party providers for quote and design services.

3. REPORTING

The following information will be required on a monthly basis to the PSI Representative.

a. Cabling Report for all locations where cable is pulled, including closet locations
b. Firestopping

4. INSTALLATION

Proposer will be responsible for the installation and warranty of equipment needed to operate the ISAAC system in compliance with the technical specifications, PSI Representative project guidelines, and agreed upon purchase order and scope of work. Equipment installation will be determined by the project management schedule and timeline.

Proposer will provide dedicated local representation of project manager(s) who work with multiple PSI Representative staff and 3rd party entities. All site surveys, project status meetings, special systems design meetings, and meetings conducted for project planning will be non-billable. Communications about schedules on all projects will be as frequent as required and will be managed in best effort. Should communications on schedules be deemed inadequate PSI Representative shall escalate a notification of infringement.

Proposer will be expected to work with several PSI Representative departments and 3rd party providers for installation services.

5. MAINTENANCE

On-site ISAAC maintenance and service support will be provided to PSI Representative for the duration of the agreement. This would include maintenance service for all equipment and software and includes, but is not limited to, spare parts, materials, labor, software, testing equipment, tools, etc. necessary to fully support ISAAC. Service and maintenance shall be available during normal business hours: Monday through Friday, 08:00 to 17:00 exclusive of federal holidays. Should PSI Representative request emergency service outside of normal business hours, said service can be provided and will be invoiced to PSI Representative upon completion of the service engagement based on the pricing agreement.

For the duration of the agreement, Proposer’s technicians shall repair or replace, at agreed upon charges and warranties, any product that fails in its described operation. Local technicians shall perform the work on site and if required, have replacement parts regularly stocked in Phoenix, at Proposer’s expense for inventory control. Technical support shall be available locally from specified and approved technical staff assigned to the project or from alternative sub-contracted personnel agreed upon by ASU to work at our Facilities. During the agreement firmware updates, software updates, and software patches shall be available from Proposer at no additional charge to PSI Representative.

Should equipment failures occur due to environmental, mechanical, or electrical conditions which fall outside of the manufacture's technical specifications for optimal system health, Proposer will repair or replace the equipment at no additional charge.

First level system support is to be provided jointly dependent upon issue by PSI Representative and Proposer. First level support includes operational troubleshooting on common end-user issues, common locking hardware issues or common server issues.

Expressly excluded from the service warranties provided for under this agreement are repair parts or services due to damage or failure of the system resulting from: misuse, negligence, accident, abuse, fire, storms, flood, wind, acts of God or public enemy, lightning or alteration by anyone other than authorized ASU staff or Proposer's technicians. Parts and/or service required as a result of the items indicated above will be invoiced to PSI Representative upon completion of the service engagement.

Expressly included in the service warranties provided for under this agreement are the repair or replacement of equipment due to defects or non-compliance to the agreed-upon technical System Design Document, and system updates as needed; included technological advancements.

Proposer will be expected to work with several PSI Representative departments and third-party providers for maintenance services.

6. EQUIPMENT PREVENTIVE MAINTENANCE

Preventative Maintenance (PM), as a component of this agreement, includes having a documented and agreed upon Maintenance Plan Document (MPD) with expected roles and responsibilities clearly outlined.

This MPD will include an equipment maintenance plan and a software (application and database) maintenance plan.

PSI Representative will receive a written report for PM duties performed by the Proposer that details maintenance performed, health status, and further recommendations for evaluation which may include costs that need to be further quoted.

7. OPERATIONAL SERVICE AND SUPPORT RESPONSIBILITIES

While the overall responsibility for the proper functionality of the ISAAC system rests with Proposer, PSI Representative will be responsible to operate the ISAAC system. Proposer will provide training to PSI Representatives so that they may operate in accordance with the System Design Document including but not limited to the following:

Proposers will provide dedicated local representation of certified Lenel Software Engineers and Service Technicians, and staff certified in Bosch intrusion hardware and Genetec video management systems in accordance with contracted services unless contract specifies otherwise.

A telephone number will be distributed to the PSI Representative for service calls when a Service Technician needs to be dispatched to the site.

When initiated, Service Technicians will schedule with the PSI Representative, arrive promptly, assess the situation, have on-hand supplies and parts, and initiate the appropriate action to provide the most capable and best-equipped onsite service support in the timeliest manner without needed follow up on-site service.

For the duration of the agreement, Proposer technicians shall repair or replace, at agreed upon charges and warranties, any product that fails in its described operation. Local Proposer's technicians shall perform the work on site and if required, have replacement parts regularly stocked in Phoenix, at Proposer's expense for inventory control. Technical support shall be available locally from specified and approved technical staff assigned to the project or from alternative sub-contracted personnel agreed upon by ASU to work at our Facilities.

A telephone number will be distributed to the PSI Representative for escalation if the local representative fails to perform within the Response Time indicated.

PSI Representative will be provided a toll-free phone number to the Proposer's Service Department to be used to request service. This is the number to be used to place all requests for service on the system. In addition, PSI Representative will be provided additional phone information that can be used in the event a response is not provided after a call has been placed to the primary toll-free number. These additional phone numbers will include the local technician assigned to the project, the project manager assigned to the project, and the Proposer's service manager.

8. REMOTE SUPPORT AND REMOTE MANAGED SERVICES (RMS)

Any Remote Support and Remote Managed Services provided by Lenel for additional service capability and integrity for all elements of the ISAAC shall be considered and negotiated annually. Lenel remote representatives are capable of providing a high-level technical assessment and assistance isolating and repairing faults within the system. The Proposer on-site representatives should be responsible for initiating the annual review a negotiation of Lenel RMS.

9. RESPONSE TIME

Proposer's local technical staff will be available to respond to a service call placed by PSI Representative. Guaranteed response time during normal business hours will be no longer than two (2) hours from the time the service call is received. Issue resolution will commence with the goal to complete the service task within twenty-four (24) hours. In most cases, issue resolution with traditional service interventions should be achieved within eight (8) hours from the time the Proposer's local technician responds. Guaranteed response time outside of normal business hours will be no longer than eight (8) hours from the time the service call is received.

Depending on the severity of the service issue or the quantity of devices involved, this timeframe may not be reasonable and consequently, the repair time may be extended. Any atypical event that will extend the repair time beyond twenty-four (24) hours will be discussed with PSI Representative and at that time an appropriate resolution plan will be developed. If parts are not immediately available locally, the fastest means of shipment will be used and the PSI Representative will have the option of locally sourcing them before the technician orders them.

10. SERVICE AND MAINTENANCE LOGS

Proposer's staff shall maintain Service Logs of all calls for service by the PSI Representative.

Proposer's staff shall maintain Maintenance Logs of all preventive maintenance and corrective repair services during the agreement period.

The Logs shall be in a format approved at time of award by PSI Representative and shall be available for inspection by PSI Representative at an agreed upon frequency and/or at any time during the agreement period, and delivered to the PSI Representative promptly. The Logs shall include a parameter driven maintenance information (by date, by comment type, by specific module, by problem type) and associated parts inventory reports. In addition, the Logs shall itemize the history of preventive maintenance and corrective/repair activities and be kept on a component-by-component basis. The Logs shall also show records of all software and hardware updates.

11. INCIDENT NOTIFICATION

Should Proposer become aware of any system incident, Lenel software bug, or any general malfunctions that prevent overall operation or a communication failure and/or the server environment lasting longer than five (5) minutes, Proposer is obligated to notify PSI Representative. PSI Representative may then have the option of posting the issue to the ASU System Health web page.

Proposer will be expected to work with several PSI Representative departments and third-party providers for service and support services.

12. OPERATIONAL, EQUIPMENT MAINTENANCE TRAINING AND ADMINISTRATIVE TRAINING

A. Operational Training

Proposer will be expected to train any and all named Segment Managers, most Area Managers, and other users on the operational functionalities of the Lenel modules as needed as a part of each installation and on-going throughout the term of the contract as non-billable service without any need for action on behalf of the PSI Representative other than to call and request to schedule the training.

Proposer will be responsible for providing training to PSI Representative and allowing and sponsoring all PSI Representative requested training from Lenel to provide certification to PSI Representative in the Lenel application for operational administration in order to operate according to the requirements in the System Design Document.

B. Equipment Maintenance Training

Proposer will provide training to PSI Representative in equipment maintenance and allowing and sponsoring all PSI Representative requested training from Lenel to provide certification to PSI Representative in the Lenel equipment and field training. This training will ensure the selected PSI Representative maintenance personnel will be adequately trained to service and install any equipment in a manner that protects the integrity of the system and the relationship with the vendor.

Proposer will provide to PSI Representative a minimum of the following:

- General training on equipment description and principles of operation
- Accessing the internal components of all field devices
- General fault isolation and troubleshooting techniques
- Standard preventative maintenance
- Configuration and testing
- Component swap-out

C. Administrative Training

PSI Representative-responsible operators will be trained and certified by Lenel in accordance with Lenel requirements for maintaining their system, allowing for direct call-in support from Lenel, and for maintaining sound business operations for optimal system health, and maintaining all information and data security.

Proposer will be expected to work with several PSI Representative departments and third-party providers for all training services.

13. TECHNOLOGY ADVANCEMENT

Proposer will provide frequent and relevant technology advancement recommendations, advice, and demonstrations throughout the term of the contract to keep PSI Representative aware of the industry solutions and enhancements of both the hardware and software components used in ISAAC.

Any new technological advances that are considered to be enhancements of functionality not obligated under this contract and outlined in the System Design Document which are requested could entail significant software and/or hardware additions and/or developments. In those instances, additional fees may be charged to the PSI Representative. Any said additional fees will be discussed and agreed upon by both parties prior to any addition and/or development.

14. LIFE-CYCLE MANAGEMENT

Proposer shall provide PSI Representative and regularly refresh a life-cycle management schedule with inventory and replacement costs. Such a plan will allow for risk mitigation and a continuous improvement plan and allow for budgeted forecasting.

Proposer shall work with PSI Representative to ensure that ISAAC shall remain sustained at a level of continual optimal health and functionality, both with respect to its hardware and software. The parties shall consult regularly as reasonably necessary to ensure that the ISAAC remains compliant and in optimal health.

15. QUALITY OF SERVICE

Proposer warrants that all of its services will be performed in a professional manner consistent with reasonably applicable industry standards and services.

16. TRANSITION PLAN

ASU's current contractor provides a turnkey service for design, installation, configuration, training, documentation, warranty, maintenance and 24/7 support for hardware and software.

A part of the transition shall be in transferring all existing transferable contracts, keys, warranties, licenses, and any components (only as current as applicable to the RFP) that are intended for operation in the current system A similar transition must be made acceptable for the release of all design builds that are in progress. No period of silence will be enforced during this process.

Transition cooperation:

Proposer agrees that it shall provide sufficient efforts and cooperation to ensure an orderly and efficient transition of services to ASU or third party supplier for a period of at least six (6) months prior to the expiration of the current Agreement. Proposer shall provide full disclosure to ASU or third party supplier, including but not limited to, equipment and services required to perform under this RFP.

Proposer will supply a sound and detailed executable transition plan describing their ability to minimize all impacts and the associated timelines for the following:

a) Software VAR key transition and joint relationship to turnkey this with current incumbent.
b) Warranty of all installs and joint relationship to turnkey this with current incumbent.
    - Door strikes, cabling, pathways, fire stops, etc.
    - Manufacturer warranty vs. installed warranty
    - Certifications of the existing installations
c) Project coordination and business service process facilitation.
    - Site surveys and walkthroughs
    - Design and engineering assistance
    - Best practice security system configuration
    - Project management and coordination

- Server and software quality control
- System documentation, user documentation, release notes, upgrades and security patch notes
- End User training
- 24/7 Service and support

d) Describe your relationship, history, and experience on transitioning work in progress.

- PO has been issued to incumbent but work has not started
- Design specs are received and approved but no PO has been delivered

List the foreseen and unforeseen risks with the transitioning of the current system and future deployment of product suites and services for the ASU systems as they exist now. Rank the value of these identified risks in order 1-5 (1 = low/5 = high) to the university.

If this award is cancelled for any reason the VAR keys must be transferred within 30 days to point of contacts designated by ASU.

17. QUALITY CONTROL PLAN

Provide a detailed quality control plan for each of the following:

Project deployment pre-install, mid install and post install

- Example: who takes ownership of the assurance of each project beginning to end
- How is it enforced
- Provide a detailed QC checklist that will be used for ASU

List all subcontractors and their associated licenses and certifications required to perform installation within the state of Arizona. Submit current registration with the state in the RFP.

List methodologies and policy and procedures including what national organization Best Practice methodologies are followed for reader configuration, biometric, cabling, server, and video.

NOTE:

- Security clearance for personnel may be required and must be submitted prior to beginning any per project work.
- Refer to Background Checks under ASU Terms and Conditions located at https://www.asu.edu/purchasing/pdf/Stand_TsCs_Provisions.pdf.
- Installation practices shall comply with industry (NEC, NFPA and IBC) and University standards.
- Projects shall be inspected and signed-off by the local jurisdiction and authorized project representative; and
- Projects shall include and follow all permit and inspection processes.

18. QUALITY CONTROL AND PROJECT MANAGEMENT SUPPORT

List the assigned Quality Control and Project Management personnel assigned to ASU and any certifications held by personnel.

List qualifications for Quality Control.

List qualifications for Project Management. Example: certifications, number of years with on-the-job experience and type of experience per user per system as it relates to Security.

Provide an example of a project plan (WBS – Work Breakdown Structure) Note:
Multiple projects require multiple Quality Control and Project Management support.

19. ACKNOWLEDGEMENT OF FINANCIAL IMPACTS

Each proposer must acknowledge that the transition of current components should not bear a financial impact on the client. Change orders, new orders, and new service requests are to become new projects and quoted by the awarded proposer.

Proposer must provide a statement of your ability to manage a full transition from the current awarded supplier on the current installed and supported system environment. The transition of services must be completed by January 17, 2020.

20. VALUE ADDED SERVICES

a) Proposer shall provide a summary of any other value added services or programs which may contribute to the overall value of your proposal, including but not limited to:

- Training
- Industry partnerships
- Support of ASU's Charter and goals
- Support of Sustainable development (including sustainability education programs), veterans' affairs, initiatives in support of women, wellness, and our changing regional demographics
- Support and enhancement of ASU's reputation as an innovative, foundational model for the New American University
- Commitment to provide significant financial and non-financial support for the University and its signature programs.

b) Proposer shall provide the ability to lease video equipment and services for video storage for special events.

c) Proposer shall provide solutions for associated security needs, such as:

- Wireless/Offline Access Control
- Intelligent Video Analytics
- Emergency Operations Centers/Security Operations Centers (EOC/SOC)
- Mobile credential
- Biometrics
- Attendance tracking
- Visitor Management
- Self Service Portals
- Web based Lenel management
- OSDP
- DataConduIT
- Other

d) Proposer shall provide white papers, guidelines, best practices, comparative analysis, peer benchmarks, documentation on new products and advanced installation, and sponsorship support for national, regional and local organizations, and advisory groups.

e) Proposer shall provide the ability to perform security reviews and provide full documentation with findings, recommendations, configurations, and pricing.

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 five (5) 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. Proposer must describe what distinguishes the ability of your firm from that of your competitors to perform the services described in this Request for Proposal.

4. Proposer must review and acceptance of ASU standard contract terms. Note: all exceptions with justification and alternative language MUST be submitted with the proposal.

5. Proposer must provide an organizational chart outlining your firm's staffing, managerial ability, and support personnel. This should include contact names and information for staff essential to the contract.

6. Proposer must provide a resume for all key personnel which details all relevant experience in the last five (5) years. Provide a brief description of the project(s), the project's overall size and scope, and their role in the project. Identify client(s) who can verify this experience and provide current contact information, including the name, phone number, email address and position of the individual who can provide the verification.

7. Provide a list of completed projects, locations and contact information for three (3) of your largest or of comparable size to ASU and of each of the following:
    a. Describe your project, scope of work, size of install
        i. System Design Diagram.
        ii. Cable and control system installations you had oversight on.
            1. Send photo examples.
        iii. Problem installs and how you overcame them.
            1. Send photo examples.
            2. Before and after if applicable

8. Proposer must provide a sample of their Operational, Equipment Maintenance Training and Administrative Training Program.

9. Proposer must provide an acknowledgement of Section XIV for ASU's Security Review Process. Note: Section XIV of the RFP is intended for proposers to understand ASU's security review processes. The proposer must understand and agree to ASU security assessment requirements if awarded this contract. This section is included only as reference.

10. Proposer must provide evidence of background check process. Background checks by Proposer must comply with all applicable laws, rules and regulations. Proposer further agrees that the background checks as required in this RFP are necessary to preserve and protect public health, safety and welfare.

Proposer Must Provide Evidence Of These Mandatory Qualifications

1. Must be authorized in the field(s) they are applying for in one or more of the platforms listed below. Proposer must provide evidence of certifications.

a. Lenel OnGuard Pro system
b. GENETEC Video Management system
c. Bosch Intrusion hardware

2. Must have the ability to provide design assistance including schematics, technical documents, and all associated deliverables including as-build.

a. Provide qualifications and final floor plan for three (3) comparable projects similar in scope and size to ASU for a door/camera design, technical documents or an as-build for each platform listed above.

b. EXAMPLE: Design example is completed within a verifiable brick and mortar facility.

c. Provide three (3) or more physical addresses of the locations within the State of Arizona if available.

d. Include the following information:
    1.) Number of Readers
    2.) Number of Cameras
    3.) A Typical Design for each of the three locations Electronic Door Hardware

3. Must have the ability to install, maintain & diagnose & support electric door hardware, alarm equipment, and security cameras.

4. Must have the ability to configure and support all Lenel OnGuard Pro software, GENETEC VMS, Bosch Intrusion hardware including new releases, updates, and integrations.

- Support calls:
    - Provide an Example of a Training Call for each of the three (3) locations.
        - Provide call description and actions completed.
    - Provide an Example of a Software or Database issue for each of the three (3) locations.
    - Provide call description and actions completed.

- Provide methodology for the following:
    - Support protocols and hours.
        - Any prioritization levels of support calls.
    - Response time.
    - Emergency contact availability.
    - Turnaround time for resolution.
    - List of Critical components available within the same business day and alternate list available within the next business day.

- Provide a list of the following:
    - Personnel that are certified Lenel OnGuard Pro proficient
    - List dates of certification and last training taken on OnGuard.
    - Methodology for continual professional growth for employees.

5. Must have the ability to configure and support Lenel Data Exchange and DataConduIT tool sets. Provide a list of integrations that have been successfully completed for other customers.

6. Must provide 24/7 support.

7. Must provide and manage a 3rd - party 24/7 call center for third party alarm monitoring.

8. Must be able to support Windows Server.

9. Must be able to support network and firewall environment.

10. Must be able to support MS SQL.

11. Must have the responsibility of oversight of installation and termination control cabling.

12. Must provide evidence of a quality control plan.

13. Must have certification of Level 3 Advanced Firestop training.

Proposers can provide evidence of these Desired Qualifications

1. Have the ability to provide online ASU specific product catalog, inventory control, warranty, service, repair and maintenance and trend statistics.

2. Provide Project Management proposed processes for doing business with ASU in each of the following:

a) Provide responsibilities of Project Manager
b) Provide responsibilities of Program Manager
c) Provide a support and escalation methodology and plan
d) Provide an ongoing-tiered customer training plan for all ASU users and technicians

3. Availability for certifications from Lenel or cooperative partners.

4. Ability to develop/conduct certification programs for user groups at ASU.

5. Provide a detailed plan for risk mitigation and continuous improvement around hardware maps, lifecycles, and maintenance plans.

6. Provide ongoing feature rich presentations and knowledge base training to campus leaders and stakeholders.

7. Provide two (2) or more Sales Representatives dedicated to ASU.

8. Provide one (1) Software Support Engineer/ Technical Engineer dedicated to ASU.

9. Provide proof of support of other Higher Education institutions using Lenel OnGuard Pro.

10. Proposer shall demonstrate how projects will be tracked.

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. Response to Section V – Specifications/Scope of Work (30%)

2. Response to Section VII - Qualifications (30%)

3. Response to Section IX - Pricing (20%)

4. Acceptance of ASU Terms and Conditions (10%)

5. Response to 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 reference 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.

Price Sheet and Guidelines
Proposer must provide the following product and service listings (include labor) in a price sheet and meet or exceed current product listings.

1. **Specify the cost of the system hardware components and installation Parts and Labor Price Sheet, using the Attachment 1 (Excel) pricing form.**

2. **Specify the cost of job pricing:**

Engineering Costs Price Sheet

SITE SURVEY	SITE CONSULTATION	DRAFTING	DESIGN/AS BUILD

Per diem / travel must be included in your totals and not separated

Project Management Price Sheet

COMMISSIONING	TESTING	COORDINATION MEETINGS	SUB/OTHER TRADE COORDINATION

ASU conducts semi-monthly coordination meetings with mandatory attendance

3. **Specify the cost of service and repair/maintenance:**

Repair/Maintenance Per Job Price Sheet

	LABOR RATE	MINIMUM
TESTING/TROUBLESHOOTING		
TRIP CHARGE		

4. **Specify the annual maintenance agreement pricing offered to clients:**

Maintenance Price Sheet

1 YEAR MAINT	2 YEAR MAINT	3 YEAR MAINT	4 YEAR MAINT	5 YEAR MAINT

5. **Specify costs for the Annual Software Support Agreement:**

Annual Software Support

ANNUAL S/W SUPPORT YEAR 1	ANNUAL S/W SUPPORT YEAR 2	ANNUAL S/W SUPPORT YEAR 3	ANNUAL S/W SUPPORT YEAR 4	ANNUAL S/W SUPPORT YEAR 5

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 hardcopy "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.

- **Confidential and/or Proprietary Information must be submitted per the instructions in Section IV, item 9. Any watermarks, footnotes, or reference to Confidential and/or Proprietary throughout the submitted proposal will be disregarded as boilerplate markings.**

- 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 per Section XIII

2. Response to Section V – Specifications/Scope of Work

3. Response to Section VII - Qualifications

4. Response to Section IX - Price Schedule and Attachment 1

5. Response to Supplier Sustainability Questionnaire

6. Review and acceptance of ASU's Terms and Conditions, Section XII. **Note: all exceptions with justification and alternative language MUST be submitted with the proposal.**

SECTION XI – Intentionally omitted.

SECTION XII – AGREEMENT - TERMS & CONDITIONS

ASU will issue a Purchase Order(s) for goods and/or services awarded under this RFP.

The parties to the Purchase Order will be bound by the ASU Terms and Conditions effective on the date the purchase order is received. The ASU Terms and Conditions are available at https://www.asu.edu/purchasing/pdf/Stand_TsCs_Provisions.pdf.

Insurance requirements are outlined within this RFP and will be included in any resulting Purchase Order. **Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed non responsive and may be rejected.** All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal.

ASU Terms and Conditions Amendment: Unless and until the District Court's injunction in Jordahl v. Brnovich et al., Case No. 3:17-cv-08263 (D. Ariz.) is stayed or lifted, the Anti-Israel Boycott Provision (A.R.S.35-393.01 (A)) is unenforceable and the State will take no action to enforce it. Offers will not be evaluated based on whether this certification has been made.

Insurance Requirements

Without limiting any liabilities or any other obligation of Supplier, Supplier 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 the Agreement, insurance against claims that may arise from or in connection with the performance of the work hereunder by Supplier, its agents, representatives, employees or subcontractors, as described below.

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

A. Minimum Scope and Limits of Insurance: Supplier's insurance coverage will be primary insurance with respect to all other available sources. Supplier 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	$5,000,000
• Products – 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 Supplier."

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 Supplier.

2. Automobile Liability. If Supplier will be driving on ASU campus or on ASU business the following section will apply: Policy will include Bodily Injury and Property Damage for any owned, hired, and/or non-owned vehicles used in the performance of the Agreement in the following amounts. If Supplier is not an individual then coverage will be a combined single limit of $1,000,000. If Supplier is an individual then coverage will be $100,000 per person, $300,000 per accident, and $50,000 property damage.

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 Supplier, involving vehicles owned, leased, hired, or borrowed by Supplier."

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 Supplier.

c. Policy will contain a severability of interest provision.

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

   a. Employer's Liability in the amount of $1,000,000 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 Supplier.

   c. This requirement will not apply to any contractor or subcontractor exempt under ARS § 23-901, when such contractor or subcontractor signs the Sole Proprietor Waiver Form.

4. Technology/Network Errors and Omissions Insurance. The terms of this section apply if: 1) ASU is purchasing or leasing software, or processing a software renewal; 2) Supplier is creating any code for ASU; 3) Supplier receives, stores, or analyzes ASU Data (including if the data is not online); 4) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data; OR 5) ASU is purchasing or leasing equipment that will connect to ASU's data network.

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

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

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

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

5. Professional Liability (Errors and Omissions Liability). If the Supplier will provide ASU Services under the Agreement, the Policy will include professional liability coverage as follows:

   - Each Claim $1,000,000
   - Annual Aggregate $5,000,000

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

   b. Policy will cover professional misconduct for those positions defined in the scope of work of the 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 Purchasing and Business Services, email Insurance.certificates@asu.edu or mail to PO Box 875212, Tempe, AZ, 85287-5212.

C. Acceptability of Insurers: Insurance is to be placed with duly licensed or approved non-admitted insurersin 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 Supplier from potential insurer insolvency. Self-Insurance may be accepted in lieu of or in combination with insurance coverage requested.

D. Verification of Coverage: Each insurance policy required by the Agreement must be in effect at or prior to commencement of work under the Agreement and remain in effect for the term of the Agreement. Failure to maintain the insurance policies as required by the Agreement, or to provide evidence of renewal, is a material breach of contract.

If requested by ASU, Supplier will furnish ASU with valid certificates of insurance. 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.** Supplier's certificate(s) may include all subcontractors as insureds under its policies as required by the Agreement, or Supplier will furnish to ASU upon request, 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 the Agreement will require the approval of ASU's Department of Risk and Emergency Management.

SECTION XIII – MANDATORY CERTIFICATIONS

Fillable PDF versions of mandatory certifications are at: https://cfo.asu.edu/business/do-business-asu under the Formal Solicitations tab. ORIGINAL signatures are REQUIRED for either version.

CONFLICT OF INTEREST CERTIFICATION

_____
(Date)

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)

FEDERAL DEBARRED LIST CERTIFICATION

Certification Other Responsibility Matters (April 2010)

_____
(Date)

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.

(D) (check one) **Have ( ) or have not ( )** within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,500 for which the liability remains unsatisfied.

(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) “Principal,” for the purposes of this certification, means an officer; director; owner; partner; or, person 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).

(b) The Offeror shall provide immediate written notice to the University 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 University 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 University 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)

ANTI-LOBBYING CERTIFICATION

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

_____
(Date)

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 University; and

(3) Offeror 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.

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

ALL SERVICE PROVIDERS ARE REQUIRED TO READ AND SIGN THIS ASU SERVICE PROVIDER ACKNOWLEDGEMENT PRIOR TO PERFORMING WORK ON ASU PROPERTY. FAILURE ON THE PART OF THE SERVICE PROVIDER TO COMPLY WITH THESE REQUIREMENTS MAY RESULT IN TERMINATION OF THE CONTRACT WITH ASU.

SERVICE PROVIDER ACKNOWLEDGEMENT

Arizona State University (ASU) is committed to protecting the health and welfare of students, faculty, staff, visitors, and to the environment. Accordingly, it is important that all members of the ASU community recognize and share this commitment and comply with the environmental, health and safety policies, rules, procedures and regulations governing ASU campus activities.

ASU is also looking to the community, including service providers, for cooperative and responsible leadership that will help the University implement a safer environment through safer practices and more sustainable solutions.

Towards this end, it is ASU's expectation that all service providers have the responsibility for environmental, health, and safety issues created or otherwise arising from or related to their work under their contract with ASU.

The service provider shall ensure that its employees are properly identified (e.g. officially issued picture ID and/or badge) and have been instructed about the boundaries of their work areas. Service providers will comply with all applicable local, state, and federal rules and regulations, including those related to the Occupational Safety and Health Act (OSHA) of 1970.

For all service providers, ASU is providing a few general guidelines in this document concerning conducting work on ASU Job Sites.

SERVICE PROVIDER DEFINITION

Refers to any individual, company, or corporation who is hired by ASU or an ASU employee to provide construction, repair or maintenance related services on ASU property or facilities.

GENERAL SITE INFORMATION

Failure on the part of the service provider to comply with the following requirements may result in termination of the contract with ASU. Prior to working in areas where site-related hazards might be present, all service providers shall consult with the project manager for more information

- Permission must be obtained from the project manager whenever it is necessary for personnel to go to the roof of any building.
- Lunch and break areas are to be coordinated through the project manager.
- Pedestrians should use walkways where provided. Shortcuts shall not be taken through operating areas.
- Explosives of any type are prohibited on the site with the **exception of powder actuated tools.**
- Barricading of ASU streets (it is required that ASU Police at 480-965-3456 must be contacted prior to any barricades being set).

- Compliance with any applicable dust control requirements are the responsibility of the service provider.

- It is the service provider's responsibility to remove excess materials, such as paints, oils, adhesives, from ASU property by the end of the project.

- Consult with the project manager and ASU Environmental Health and Safety (EHS) if the project will involve regulated ASU waste, such as potentially contaminated soil, light bulbs or oil.

- Chemicals, paints, oils, fuels, etc. must be located so as to avoid potential contamination of storm drains and dry wells. The project manager will assist with determining the appropriate location.

PARKING (Park in specified areas only)
The proper parking permit must be secured from ASU Parking and Transit Systems (PTS) and displayed appropriately in vehicles. Contact the project manager and/or PTS at 480-965-6124. Do not block entrance ramps, trash docks, and truck doors, etc.

LOCKOUT/TAGOUT
ASU has established very specific control measures related to the control of potentially hazardous energy referred to Lockout/Tagout/Verify for all maintenance and construction related activities at ASU facilities. Each service provider conducting similar activities must adhere to all requirement of the ASU program which mirrors the OSHA Standard 29 CRF 1901.147 as posted on our website (Workplace Community Safety) with the exception of the service provider's designated lock. Each service provider is required under OSHA regulations to have their own program meeting the standards requirements, but all requirements in the ASU program with the exception of lock color and style must be met including notification of all affected personnel of the Lockout/Tagout/Verify activity, logging activities, and transitioning to equipment out of service. Service providers may be required by their project manager to post notices identifying their designated locks. At no time may Lockout/Tagout devices be used for equipment out of service.

ELECTRICAL SERVICES
Work on live electrical services at 50 volts or higher is prohibited unless permitted through your project manager under the ASU Electrical Safety Program. All work on electrical services must be locked out as required under 29 CFR 1910.147.

DISCLOSURE OF ASBESTOS, LEAD AND/OR OTHER HAZARDOUS MATERIALS

ASU is informing all service providers of the potential presence of asbestos (e.g. which may be found in caulk, sheetrock joints, vinyl tiles, etc), lead, and/or other hazardous materials at ASU. Depending on the location(s) of your work, there may be one or more of these materials present. It is your responsibility to discuss the full scope of your work with the project manager or designee so that you have the appropriate information related to asbestos, lead and/or other potentially hazardous materials. If the scope of your work changes, contact your project manager or designee before proceeding to determine if the change in scope may involve the potential disturbance of asbestos, lead and/or other hazardous materials.

Should there be changes to your scope of work affecting areas outside of your original contract area, or, if unforeseen or unidentified suspect materials be uncovered or discovered during your work, you are required to stop all work which would impact those materials until they can be evaluated and tested by ASU. Immediately upon discovery of any unidentified or unforeseen building material, you must notify the project manager to arrange for ASU to evaluate and test the materials.

Prior to your work taking place, inspections for asbestos, lead and other potentially hazardous materials must be (or have been) conducted by ASU, and identified materials (containing asbestos, lead or other hazardous materials) that would be disturbed by your current scope of work will be (or have been) removed or isolated in such a manner as to prevent potential exposure. Please contact ASU Asbestos Program Manager at 480-965-7739 to determine if, based on your current scope of work, there any remaining materials which are or may be present in adjacent location(s), but should not be disturbed.

Your signature on this document acknowledges you received this disclosure and that you had the opportunity to review your scope of work with the project manager or designee.

The **Service Provider Job-Site Safety Information** orientation document is meant to serve as a guide for the service provider, any and all of its supervisors, and any and all of its subcontractors during their performance within the scope of work under their contract with ASU. Although the document sets forth certain guidelines and rules of operations on ASU sites, it is not intended to address every potential safety and health issue that may arise during the scope of the contracted work. **IT DOES NOT COVER EVERY POSSIBLE SITUATION**.

While ASU retains the right to periodically review the work of any service provider, its supervisors, or its subcontractors, ASU does not assume responsibility for any issues identified outside of contract compliance.

TEMPE CAMPUS UTILITY TUNNEL SYSTEM

Asbestos exists in the underground utility tunnel system located on the Tempe Campus of ASU. It is your responsibility to discuss the scope of your work with the project manager or designee in order to provide you with any further information related to asbestos issues which may be encountered during any work in the tunnels.

The gravel or earthen flooring material throughout the tunnel system has become contaminated material from historical damage and repair to pipe insulation. Walking on, or other disturbance to, the flooring material may cause entrained asbestos fibers to become airborne.

In addition, asbestos is present in most thermal system insulation applied to steam, steam condensate and hot water piping. The disturbance of insulation materials is strictly prohibited.

ASU has determined that persons working in the underground utility tunnel system may be potentially exposed to airborne asbestos fibers at or above the OSHA permissible exposure limit of 0.1 fibers per cubic centimeter (f/cc).

Service providers are advised that airborne fibers which exist in the tunnel areas may be below the minimum length of five microns capable of being detected by analysis using Phase Contrast Microscopy (PCM) analytical techniques. Airborne fibers within the tunnels are detectable using Transmission Electron Microscopy (TEM) methods. Each service provider is responsible for ensuring proper use of personal protective equipment including respiratory protection at all times while working in the Tempe tunnel system.

Contaminated waste materials generated by use of such personal protective equipment are required to be appropriately packaged in Department of Transportation-approved and labelled asbestos waste bags. Bags are to be removed from ASU property and properly disposed at the end of each work shift. Bags staged to accept waste are required to contain visible labels that clearly identify the name of the firm generating the waste, contact phone numbers, the dates, where the waste was generated, and the ASU project number.

It is your responsibility to discuss the scope of work conducted within the tunnel system with your employees, or sub-contracted employees, and to provide the appropriate training, personal protective equipment and air monitoring as required by OSHA.

POLYTECHNIC CAMPUS
The Polytechnic Campus is subject to specific excavation requirements. Contact EHS at 480-965-1823 if the project involves excavation at the Polytechnic Campus.

Accordingly, ASU expects each service provider to supplement the provisions contained in the Service Provider Job-Site Safety Information & Guidelines Orientation document with proper instructions and work practices that, based on knowledge and experience, will help decrease the likelihood of injury to service provider employees, subcontractors' employees, and to others, as well and prevent damage to property and material on ASU sites.

[Service Provider Name]_____

[Street Address]_____

[City, State Zip]_____

The above service provider certifies that they, any and all of its subcontractor's, or its supervisors, prior to commencing any work on an ASU site, have reviewed and understand the contents of the Service Provider Job-Site Safety Information & Guidelines Orientation document located at EHS Safety Manual and/or have attended the Service Provider Job-Site Safety Information & Guidelines orientation program produced by ASU Environmental Health and Safety. By having their representative sign and date this document prior to commencing any work, the service provider accepts, and agrees to the provisions of these Acknowledgement Clauses.

[Name]_____

[Title]_____

_____

Employer Representative Signature Date

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.

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.
Arizona State 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 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?

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. Arizona State 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 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

3. What is your firm doing to be energy efficient?
4. 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])
5. What plan is in place to reduce greenhouse gas emissions in the future?

Solid Waste

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

Water Waste

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

Packaging

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

Sustainability Practices

11. What programs does your firm have to encourage your employees to use alternative transportation while commuting to work and travelling locally?
12. What sustainability guidelines or environmental statement does your firm have to guide the firm as a whole?

13. What are your firm's sustainable purchasing guidelines?
14. What kind of position(s) or team(s) does your firm have dedicated to overseeing sustainability initiatives?
15. List the sustainability related professional associations of which your firm is a member.
16. What kind of effort does your firm make to reduce the use of environmentally harmful materials?
17. Has an environmental life-cycle analysis of your firm's products been conducted by a certified testing organization?
18. Does your firm use Green Seal/EcoLogo certified or biodegradable/eco-friendly cleaning products?
19. Has your firm been cited for non-compliance of an environmental or safety issue in the past ten years?
20. Name any third party certifications your firm has in regards to sustainable business practices?
21. Describe any other initiatives your firm has taken to integrate sustainability practices principles into your operations.

Community

3. What charity, community development, educational programs, or environmental programs is your firm involved in within your local community?
4. 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

SECTION XIV - SECURITY REVIEW (REFERENCE DOCUMENT #1)

Security Review Form
Form version: 2017-04-13
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 -- in this checklist and in your Security Architecture Worksheet (example here) -- 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 use ServiceNow to submit a request for a security review.

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?

☐ This project is not using Planview.

What is the purpose of your project? Briefly describe the business problem you are trying to solve.

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?

☐	High	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. If the vendor has signed or has intent to sign the ISO contract language ensure you provide a copy of the following documents from the vendor: SOC2 Report System Development Life Cycle (SDLC)
☐	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.)

☐	High	Sensitive data will be traveling across one or more external connections outside of the ASU data Center 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.)

☐	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: this is a detailed technical diagram specific to your implementation at ASU. Vendor diagrams are usually NOT 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 also required. It can help you gather the information needed for your diagram. You should find a blank worksheet in your security review folder. The information in your worksheet should match your diagram and vice versa.

Has a complete security architecture diagram been submitted?

☐	Unknown	***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.*** 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	***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.*** 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 in the boxes below. (Note: A DNS name is not a URL. URLs for web servers are requested in a different question.)

Your Security Architecture Worksheet (example here) should already have 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: ASU managed only - 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. Your Security Architecture Worksheet (example here) should 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.

NOTE: ASU managed websites only - To request a web scan submit a web application scan through the MyASU Service tab (or here: http://links.asu.edu/requestascan).

☐	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. ASU has received 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://links.asu.edu/webapplicationsecuritystandard.

☐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?

☐	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?

☐	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	Passwords are stored in a way that if obtained by a hacker, the hacker could use them to log in. For example (1) the plain text of the password is stored, or (2) the password is encrypted at rest but the encryption could be reversed to obtain the plain text of the password.
☐	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	Access is in compliance with the ASU Privileged account standard: https://docs.google.com/file/d/0B7bqVGx3GJQbaC10bEl0ZndjVVE/
☐	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?

☐	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.

However if you contract with Vendor A and they subcontract with Vendor B, ASU may not require a contract directly with Vendor B. Vendor A may be responsible for Vendor B.

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	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?

☐	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 http://links.asu.edu/webapplicationsecuritystandard 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?

☐	HIGH	No logging is performed on any system
☐	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?

☐	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 (http://links.asu.edu/softwaredevelopmentlifecycle) 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?

☐	High	No vulnerbility scanning or penetration testing has been conducted
☐	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?

☐	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					

Risk Acceptance

After your documents are complete and the review discussion has been held, someone will be asked to accept any remaining risk. Please be aware that if your Risk Score includes any Red items, the ASU Provost or CFO will be asked to accept the risk. Orange items go to the sponsoring business unit's Dean or comparable leadership for risk acceptance. Low risks may be accepted in writing by a member of the project team.