ASU Arizona State University

December 16, 2019

REQUEST FOR PROPOSAL

MANAGED PRINT SERVICES

RFP 342006

DUE: 3:00 P.M., MST, 1/31/20

Deadline for Inquiries	3:00 P.M., MST, 1/10/20
Time and Date Set for Closing	3:00 P.M., MST, 1/31/20

TABLE OF CONTENTS

TITLE **PAGE**

SECTION I – REQUEST FOR PROPOSAL

RFP 342006

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Managed Print Services.**

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 & Broadway Road) Tempe, Arizona 85281 **on or before 3:00 P.M. MST January 31, 2020** at which time a representative of Purchasing and Business Services will announce publicly the names of those firms or individuals submitting proposals**.** All times noted are Mountain Standard Time (MST). Please note that Daylight Savings Time is NOT observed. 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**. **No proposals will be accepted after this time.** No other public disclosure will be made until after award of the contract.

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

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

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

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

ARIZONA STATE UNIVERSITY

____
Lorenzo Espinoza
IT Strategic Sourcing Manager

LE/SK

SECTION II – PURPOSE OF THE RFP

1. INTENT

Arizona State University is seeking proposals from qualified vendors interested in providing Managed Print Services as outlined in this RFP. Managed Print Services, at a high level, includes the provision and management of both single and multi-functional print and/or scan devices across the Arizona State University campus. The goal of this RFP is to work towards solutions that will minimize cost (both direct and indirect), promote the centralization of print devices, develop process efficiencies, and create a sustainable solution that minimizes ASU's footprint as it relates to overall resource consumption.

2. BACKGROUND INFORMATION

Fleet Makeup/Volume

Arizona State University has Managed Print Services through one strategic vendor (hereinafter referred to as the "SV") relationship and has worked with the SV to ensure each department is right-sized according to its needs and actual output. Provided below are estimated figures with regards to Arizona State University's overall fleet makeup and annual clicks/prints for devices that are managed:

Managed Devices		
Description	**Single Function**	**Multi-function**
Black and White (B&W)	38	361
Color	45	305

Managed Click/Print Totals	
B&W	142,258,703
Color	33,494,061

Arizona State University recognizes that there is opportunity to further centralize its print fleet and welcomes vendor recommendations to reach this potential. Provided below are the estimated quantities of devices that are not managed:

Unmanaged Devices			
Description	**Single Function**	**Multi-function**	**Unknown**
B&W	587	283	90
Color	419	481	165

High-Level Managed Print Services Operational Current State

The following provides a high level overview of what the operational framework looks like within the Managed Print space:

- SV provides equipment, delivery, installation, configuration, toner supplies and delivery, preventative maintenance, parts, repairs, and decommission and removal of devices
- SV provides periodic print assessments to optimize the fleet and support a more sustainable environment

- Detailed reporting provided by SV to document usage and fleet makeup by device, location, age, etc.
- Various Service Level Agreements related to operational and service efficiency provided by SV to track success of program
- Spent SV-specific toner cartridges collected, packaged, and shipped by ASU to SV for recycling
- ASU orders paper and SV delivers to device locations. SV reimburses ASU for each paper order.
  - All paper ordered for managed devices are required to be comprised of 100% recycled content
- ASU provides front line customer support for public print (i.e. classrooms) devices and triages device issues to SV; SV is contacted directly for device issues within the office setting
- SV orders and delivers toner to devices under management contracts
- ASU provides hardware and software infrastructure support to include server support (management of Pharos, server housing, OS management, troubleshooting)
- Routine collaboration between SV and ASU to discuss ongoing challenges and successes, and development of action plans for addressing key issues
- Onsite dedicated SV account manager
- Orders for new devices are directly submitted from a business unit within ASU to SV
- Individual purchase orders are issued by each ASU department for lease and click/print costs
- Billing for leased devices and click/print allowances occurs at the beginning of each contract year; overages are paid at end of each contract year
- Equipment is generally leased with varying click/print allowances per device type
- Leases are primarily five (5) years
- Total lease value left as of the issuance of this RFP is approximately $5.4 million, and an estimated $4.4 million left as of June 30, 2020 is projected
  - The figures represented above assume that there are no changes (i.e. additions) to the current devices makeup, which is highly unlikely and not representative of future state
- SV provides financial support for ASU personnel to support the overall program (i.e. account management, IT support, etc.), marketing, leases, and profit sharing.
- Quarterly and semi-annual reviews are conducted to review the financial and operational status of SV, performance related to the SV's service level agreements and other KPIs, and how the SV has been integrated within the campus community

General

Arizona State University is a new model for American higher education, an unprecedented combination of academic excellence, entrepreneurial energy and broad access. This New American University is a single, unified institution comprising four differentiated campuses positively impacting the economic, social, cultural and environmental health of the communities it serves. Its research is inspired by real world application blurring the boundaries that traditionally separate academic disciplines. ASU serves more than 98,000 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 at http://www.asu.edu.

3. TERM OF CONTRACT

The initial contract term will be for five (5) year(s). 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

All times noted are Mountain Standard Time (MST). Please note that Daylight Savings Time is NOT observed. 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 Road 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(s) 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. The University reserves the right to award all or part of this RFP to one or more suppliers at its sole discretion.

10. The University reserves the right at its sole discretion to share this RFP and its results with other public universities, and with public Procurement Cooperatives to which the University is a member, for the purposes of utilizing the award for their own contract.

a. Any resultant contract between awardee(s) and other public universities or public Procurement Cooperatives is solely between those two parties. Awardee(s) are under no obligation to honor pricing or terms resulting from a negotiated contract with ASU.
b. Awardee(s) will be required to pay the University a 2% annual administration fee based on total net revenue from any public university or public Procurement Cooperative utilizing the results of this RFP as their own award.
c. The administration fee may be charged by the supplier directly to other public universities or public Procurement Cooperatives

11. Other public Arizona entities, including but not limited to, Northern Arizona University, University of Arizona, and Maricopa County Community College District may use the award and contract resulting from this RFP.

12. **Central Receiving and Last Mile Distribution Fee for real goods shipped to the University:** ASU operates centralized receiving warehouses that will be used for the majority of campus deliveries. The University's Central Receiving Unit will charge a fee to the supplier for all centralized shipments in the form of a Last Mile Distribution Fee.

a. This fee can, in turn, be billed back to the University in the cost of goods or added as a separate delivery fee.
b. This fee, totaling 5% of the gross funds paid to the Supplier, shall be paid directly to the Centralized Receiving Unit. This fee will apply to any and all products sold by the Supplier that are delivered to Central Receiving.

The Fee will be calculated based on all sales transacted. The Supplier will submit the Fee, along with quarterly reports documenting all sales, to the University within 30 days following the end of each calendar quarter. Each quarterly report shall include, as a minimum, all purchased goods, price paid, and quantity for all sales within the calendar quarter just ended. Other options for last mile compensation can be discussed in the proposal, but responses should include acknowledgement of willingness to engage.

13. 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. Any watermarks, footnotes, copyright or reference to Confidential and/or Proprietary throughout the submitted proposal will be disregarded as boilerplate markings.

14. 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.

15. 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.

16. **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.

17. 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.

18. 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.

19. 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.

20. 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 10 days from the date of the award.

21. 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.

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

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

Tel: 480-965-3849
E-mail: Lorenzo.Espinoza@asu.edu

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

Note that the University will not 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.

Proposers are prohibited from communicating directly to any member of the RFP committee other than the named Buyer during the RFP process except those activities conducted under the committee's purview. Participants with other business with the University that does not fall under the purview of this RFP may conduct that business as would normally be required to maintain that business.

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 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.

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

SECTION V – SPECIFICATIONS/SCOPE OF WORK

Arizona State University is seeking a comprehensive managed print provider to perform the following services. Please indicate your ability to provide the following services.

1. **Print Assessment & Optimization** - Contractor will collaborate with ASU offices to ensure it maintains sustainable print and document handling processes and environments. Contractor will perform routine print assessments and monitoring to determine the cost of the current print environment, identify areas of opportunity for savings and creating a more sustainable solution, and maximize device performance.

2. **Equipment** - The awarded vendor ("Contractor") will provide single and multi-functional print devices and any applicable peripherals that may either be purchased or rented as determined by ASU. All devices must be new unless otherwise agreed by the parties in writing.

3. **Print Management System** – Contractor will provide a print management system capable of copying, printing, and scanning. Contractor will assist departments to attain their departmental goals, such as tracking cost centers, and customized print strategies, roadmaps, and reporting. The print management system shall be secure and capable of controlling variables such as single vs. duplex printing.

4. **Installation** - Contractor will be responsible for delivery and installation of all managed devices and peripherals. Contractor will be responsible for taking back (removing from ASU premises) all pallets and packaging related to delivery and installation.

5. **Management of Devices** – Contractor will provide managed services for the single and multi-functional print devices provided by Contractor to ASU, as well as any devices owned by ASU that can reasonably be managed under Contractor's services. All devices managed under the awarded contract shall be maintained by Contractor, to include, but not limited to:

   5.1. Ensure devices remain operable and within the conditions of any negotiated service level agreements (SLAs)
   5.2. Provide preventative maintenance to the managed devices according to the manufacturer specifications
   5.3. Provide all consumables (including toner and parts, but excluding paper)
   5.4. Repair the managed devices as needed
   5.5. Provide the appropriate security measures to ensure secure printing and the safekeeping of ASU data. All devices managed by Contractor must use an industry standard encryption protocol for data in transit and at rest. Contractor will perform periodic scanning and penetration tests for any unauthorized access or systems vulnerabilities.
   5.6. Provide asset tracking and reporting on active/decommissioned equipment. For each device, Contractor shall provide monthly reporting on the serial number, model number, agreement number, purchase date, install date, rental termination date, number of months remaining on rental, total value of the remaining rental term, retail price, purchase price (including discounts, rebates, credits, promotions and the like, whenever applied), current deployment status and location, ASU property control number (if applicable), click/print volumes, and vendor end-of-support date, in an editable format (xls or csv preferred). In addition, Contractor will, on a monthly basis provide ASU with a report identifying all purchases, rentals, and deployments made in such month.
   5.7. Provide monthly reporting that outlines other areas (not specifically related to print services) where the Contractor may be engaged with ASU with the intent of fostering community engagement and supporting ASU's charter and goals

5.8. Relocation and Removal of Devices – Contractor will relocate devices as requested by ASU, as well as remove the devices from ASU campuses that reach the end of their contract term or useful life and erase or destroy the hard drive. Contractor will perform data erasure services for such equipment using a method consistent with NIST Guidelines for Media Sanitization, Special Publication 800-88, Revision 1, at a level of "purge" or higher.

5.9. All services shall be performed during ASU's normal business hours (8:00 A.M. to 5:00 P.M. Monday through Friday, excluding holidays).

6. **Service Level Agreements** - All Services shall be performed in accordance with the service level agreements described by the Contractor in their proposal or as otherwise negotiated between the two parties.

7. **Account Management** – Contractor shall provide at least one onsite account manager responsible for the overall program. Both ASU and Contractor shall also form a team to meet on a periodic basis to discuss objectives, develop roadmaps for those objectives, and strategize on areas of opportunity.

8. **Miscellaneous**.

8.1. ASU currently supports and maintains on-premises print management software. To advance our cloud-first strategy ASU prefers print as a service or cloud-based alternatives. Describe the strengths and weaknesses of your available alternatives, your recommended approach, and how each model would be implemented and supported.

8.2. Describe any significant task not listed in the Specifications/Scope of Work which are known to be necessary under the proposed agreement.

8.3. ASU may add to the Specifications/Scope of Work or make changes in the Specifications/Scope of Work for services of a similar nature to those specified in this Request for Proposal as mutually agreed to at a price mutually agreed upon. The change must be approved by the Procurement Officer and a contract amendment issued by the Purchasing office to change the contract.

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.

Experience

1. The proposer must present evidence that the firm or its officers have been engaged for at least the past ten (10) years in providing services as listed in this Request for Proposal.

2. The proposer must present evidence of a minimum of ten (10) years of experience providing managed print services to accounts of similar size and scope to that of ASU.

3. The proposer must provide who the single point of contact for managing the entire printer environment, project, and eventual Agreement will be, as well as include his or her resume.

4. The proposer must certify their ability to be able to lease, maintain, and support the OEM Brand MFD included in its proposal. If the proposer is using a servicing entity then the servicing entity must be provided in their proposal.

Operational Processes & Strategy

1. The proposer must describe their process of conducting a Printer Fleet Assessment both at the beginning of the contract and throughout the lifecycle of the agreement.

2. The proposer must describe their recommendation for addressing the number of devices that are currently under active leases and the best approach to ensuring there is no significant disruption in services and that any financial obligations tied to active leases are appropriately addressed.

3. Describe your approach to developing a best practices strategy to be shared from site to site to foster improvement at all campus locations

4. Specify how you will handle any device with a high number of service calls (“Lemon” clause)

5. Specify availability of parts, components, and consumables (consumables will not include paper) and how you plan to monitor and fulfill the needs of each device.

6. Describe your process for printer moves within ASU’s network and the support provided.

7. Describe your recycling infrastructure and processes for recycling toner cartridges, de-commissioned devices, and packaging.

Centralization Efforts

1. Currently, ASU works within a distributed model where devices are requested and approved directly by each department. The proposer must describe their plan for getting individuals not currently within the managed network to “buy into” the centrally managed concept.

2. The proposer should describe their approach to reducing the number of old and obsolete printers to: (a) reduce energy costs; (b) reduce maintenance time and expense; (c) migrate non-contracted devices to the company's OEM products, and; (d) reduce desktop printers in favor of MFDs.

Account Management & Service Level Agreements

1. Describe the individuals that would be assigned to support this agreement to include onsite vs. offsite personnel and level vs. remote support. Please also include your escalation path for resolving issue.

2. Please indicate how you define success in an overall managed print concept, and the process for creating campus locations and site specific (e.g. building location) process benchmarks from which to monitor and adjust, preferably through an online executive dashboard.

3. What quality assurance metrics do you implement to measure personnel and devices performance and how do you act upon those metrics to ensure customer satisfaction?

4. The proposer must describe their Service Level Agreements, including but not limited to:

   a. Hours of operation
   b. Phone and Email support options
   c. Tier escalation response definitions and times
   d. In addition to 9.c., describe your performance categories based on acknowledgement time, response time, and resolution time per the below definitions:
      - Acknowledgement time: indicates time to acknowledge maintenance and support requests through email, phone, or system used for tracking and managing incidents. Acknowledgement includes written confirmation.
      - Response Time: indicates time to accept, arrive onsite, and begin work on service requests providing no security/access delays or extreme circumstances beyond control of vendor.
      - Resolution Time: indicates time to resolve the problem stated on the ticket with a start time beginning at initial escalation and assignment. Closing/resolution includes all items that are within scope of vendor responsibilities
   e. Specify your current average and maximum response time across your current clients and how response time is calculated
   f. Provide the software and hardware uptime guarantees you are able to provide
   g. Provide any remedies or penalties that you provide for missing any of the SLAs discussed in this proposal.

Reporting

1. Please indicate if you provide a client-accessible solution for accessing reports related to the overall print program.

2. Indicate what reportable features are available to your client and in what format. Examples may include, but are not limited to:
   a. Number of audited devices by month, week, and day
   b. Managed vs. non-managed devices on network
   c. Identifying color vs mono devices
   d. Manufacturer
   e. Model
   f. Serial Number

g. IP address
h. Location of device (identified during initial audit)
i. Remote meter reading per month (providing view of current supply levels) for billing and utilization purposes
j. Number of monochrome and color pages, per device and in aggregate
k. Number of simplex and duplex pages, per device and in aggregate
l. Number of jobs, per device and in aggregate
m. Provides access to service ticketing and history
n. Provides ability to place service call
o. Knowledge Base – Provides a searchable knowledge base of common service issues per model & corresponding resolutions 24/7/365.
p. Department liaison for device
q. Number of service calls per device
r. Mean time to resolution per time
s. Consumable usage
t. Part replacements and other repairs documented
u. Itemized incidents with creation date, acknowledgement, response, and resolution times
v. Allowance and usage difference, per device and in aggregate
w. Utilization rates by device and fleet averages (percent of time in use, in sleep mode, etc.)
x. Actual energy use per device and total fleet energy usage by month
y. Average downtown/uptime

Implementation & Training

1. Please describe your general approach and ideal implementation plan for managed print program of this size and scope.

2. Please provide a list of devices that you are recommending in response to this RFP. Please include with the list of devices the manufacturer, model number, standard input tray size, duplexing capabilities, optional accessories and peripherals, pages per minute, energy usage, internal memory, monthly duty cycle, and sustainable certifications for each device.

3. The proposer must describe their complete training program for end users. ASU is highlighting the importance that the successful proposer includes training for the entire staff and/or new staff and that every staff member will be equipped with the knowledge of how to use the new technology. Initial training of ASU personnel will be conducted upon equipment installation and at no cost to ASU.

4. The proposer must provide a Gantt chart (a preliminary project schedule) to identify the estimated timelines of the project, the roles and responsibilities between the awarded proposer and ASU, and any additional resources needed for the project. This project plan must include an installation timeline and proposed project milestones that matches as close as possible to all components outlined within Section V Specifications/Scope of Work and this Section VII Proposer Qualifications.

Security & Access

1. The proposer must provide details of their ability to allow users to connect to copier/printer/e-mail/LAN faxing functions from their desktops/laptops/tablets/smartphones/devices efficiently and with confidentiality options.

2. What security controls do you typically put in place to ensure print jobs are completed securely?

3. What security controls do you use to identify potential security threats to servers?

4. If not addressed above, please indicate how an employee or student can access their print jobs on the device (i.e. id card, security code, etc.).

5. The proposer must describe the security measures that are used to ensure that sensitive data is not insecurely transmitted, stored, or collected (ex. Wiping of drive/purging data).

6. The proposer must describe how data will be purged from old copiers and printers.

Sustainability

1. The proposer must be able describe their plan to reduce paper consumption by duplexing, where applicable, as standard functionality for all print platforms.

2. The proposer must describe their plan to reduce the total number of copies and print jobs needed over time.

3. The proposer must describe their sustainability programs and procedures, if any, that their company has in place, including their supply recycling program, device recycling, use of recycled materials in the manufacturing of devices and supplies, and packaging take-back program.

4. The proposer must explain if any small businesses will be utilized as part of this contract.

5. The proposer must provide energy usage information on the five most prevalent devices they are proposing to deploy.

6. The proposer must verify whether any of the proposed equipment have an organic photoreceptor. If not, detail whether the proposed equipment contain any hazardous materials such as arsenic, cadmium, or selenium.

7. The proposer must specify whether the proposed equipment contains polybrominated diphenyl ethers (PBDEs) and polybrominated biphenyls (PBBs).

8. The proposer must indicate to what level its equipment falls within certain sustainability certifications, including, but not limited to EPEAT (Gold, Silver, or Bronze), Energy Star, and other equivalent certifications. The proposer must also state how it is able to report on its certifications related to the use of each device.

9. The proposer must describe their plan to maximize the resale value from existing equipment that will be disposed or demonstrate that any equipment not resold will be recycled through a vendor certified under the e-Stewards® and/or Responsible Recycling (R2) standards.

10. The proposer must describe how it supports efforts to increase usage of paper comprised of 100% recycled content in lieu of less sustainable paper options.

Value Added Services & Financial Statements

1. The proposer should provide details of their Value Added Services as part of the strategic initiative of this RFP. Please 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:
    a. Training

b. Industry partnerships
c. Support of ASU's Charter and goals (such as research, education and/or community embeddedness relationships, internships and recruiting, diversity and inclusion, etc.)
d. Support of Sustainable development, veterans' affairs, initiatives in support of women, wellness, and our changing regional demographics.
e. Support and enhance of ASU's reputation as an innovative, foundational model for the New American University.
f. Support of ASU's sustainability goals (carbon offsets, water offsets, tree plantings, etc.)
g. Commitment to provide significant financial and non-financial support for the University and its signature programs.
h. Any other goods or services your company provides

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) hard copy and one (1) soft/digital copy (e.g. flash drive) 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) hard copy and one (1) soft/digital copy (e.g. flash drive) in a separate sealed envelope and mark as follows:

(Firm's Name)
Confidential – Financial Statements

Terms and Conditions & Security Reviews

1. The proposer must provide a statement of their review and acceptance of ASU's Terms and Conditions included in this RFP under Section XII. **Note: all exceptions with justification and alternative language MUST be submitted with the proposal.** In no event is a Proposer to submit its own standard contract terms and conditions or a previously negotiated ASU contract as its sole response to this section.

2. The proposer must provide a statement of 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.

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 Specifications/Scope of Work (25%)

2. Response Pricing Schedule (25%)

3. Response Proposer Qualifications (25%)

4. Response to ASU Terms and Conditions (15%)

5. Response to 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. ASU is currently contemplating varying cost models and requires the Proposer to submit pricing for each pricing model displayed below. In all cost models, Proposer should assume that Proposer will be responsible for all consumable costs (excluding paper). Optional accessories and equipment associated with each device should be clearly stated underneath each device and priced accordingly. In each pricing model, pay-for-print devices must be included and clearly identified in each cost model. Pay-for-print devices costs must include all consumables, inclusive of paper. The list provided in your pricing schedule is a list of potential units that may be modified through the duration of the overall Agreement. ASU reserves the right to add or remove individual devices from the Agreement at any time.

Lease plus Pay per Click/Print Cost Model

The following cost model requires Proposer to provide a lease cost by varying term lengths. In addition, a per click/print cost should be provided that would include the cost of maintenance/management and consumables (excluding paper for non-pay-for-print devices). No click/print volumes should be included in this price model.

Model Number	**Description**	**Lease Cost per Term Length (Months)**			**Click/Print Cost**	
		36	**48**	**60**	**B&W**	**Color**

Lease plus per Monthly Maintenance Cost Model

The following cost model requires Proposer to provide a lease cost by varying terms. In addition, a monthly maintenance cost should be provided that would include the cost of maintenance/management and consumables (excluding paper for non-pay-for-print devices). If there is a click allowance for each device, please include the allowance in the appropriate column. If applicable, Proposer must indicate the overage costs on a per click basis if the monthly click allowance is exceeded.

Model Number	**Description**	**Lease Cost per Term Length**			**Monthly Maintenance Cost**	**Monthly Click Allowance**	**Click/Print Overage Costs**	
		36	**48**	**60**			**B&W**	**Color**

Pay per Click/Print Only Model

The following cost model requires Proposer to provide pricing on a pay per click/print basis only. The pay per click/print must include the cost of the device, maintenance/management, and consumables. ASU prefers no volume commitments in this model. However, if necessary, Proposer should indicate if there are any volume expectations/commitments that accompany this model.

Model Number	**Description**	**Click/Print Cost**	
		B&W	**Color**

General Pricing Questions

1. ASU currently permits each department to submit device requests, orders, and payment directly to the SV. What is the impact on the cost models addressed above if ASU switched to a more centralized model where requests, orders, and payment are streamlined through one department?
2. ASU currently pays for its device lease and maintenance costs at the beginning of each year, and reconciles payment for any pay-for-click devices or overages at the end of each year. What is the impact on the cost models addressed above if ASU switched to monthly reconciliation model?
3. As mentioned previously, SV provides financial support for ASU personnel to support the overall program (i.e. account management, IT support, etc.), marketing, leases, and profit sharing. Please indicate if you are including any of these elements in your proposal and provide a detailed description of each.
    a. How does the inclusion of the financial support impact the costs models addressed above (please include the impact on cost as a percent)?
4. If not addressed above, please indicate what your revenue share program would look like if awarded the services in this RFP.
    a. How would a revenue share program impact the cost models addressed above (please include the impact on cost as a percent)?
5. Due to the need to be more sustainable and ASU's support for the reduction of resource consumption, ASU anticipates that there will be a need to modify or remove devices. Is the Proposer willing to provide an annual allotment for changes or removal of devices? If so, please explain.
    a. How else is the Proposer willing to provide greater flexibility to accommodate changing needs and technology advances?
6. As mentioned previously, ASU desires to evaluate the benefits of moving to a cloud-based model vs. on-premise. Please explain any impact on costs that ASU should consider in its evaluation.

SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS

Format of Submittal

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

1. **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

2. **One (1) “single”** continuous electronic copy (**flash drive only**), PC readable, labeled and no passwords.

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

4. 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. Appendix 1 – RFP Checklist/Cover Page

2. Response to Section XIII – Mandatory Certifications & Supplier Sustainability Questionnaire

3. Response to Section VII – Proposer Qualifications (Maximum 20 pages not including Exceptions, Justification and Alternate Language to Terms and Conditions, resumes, CVs, and/or Organizational Charts. Do not include Financial Statements – see below).

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

5. Response to Section IX – Pricing Schedule

6. Financial Statements per Section VII

7. Confidential/Proprietary Justification Letter with Sealed documents, if applicable. Please review instructions under Section IV, page 9, item 9

SECTION XI – PROPOSER INQUIRY FORM

Pre-Proposal Questions, General Clarifications, etc.

PROJECT NAME: ____

PROPOSAL NUMBER: ____

INQUIRY DEADLINE: ___3:00 P.M., MST, January 10, 2020___________________

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

DATE: ____________________________

WRITER: ____

COMPANY: ____

E-MAIL ADDRESS: ____

PHONE: ____________________________ FAX: ________________________

QUESTIONS:

____

____

____

____

____

____

____

____

____

____

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 ASU Standard Terms and Conditions.

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	$2,000,000
• 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	$5,000,000
• Annual Aggregate	$5,000,000

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	$2,000,000
• Annual Aggregate	$2,000,000

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.

____

____
(Email address)

____
(Signature required)

____
(Print name)

____
(Print title)

____
(Address)

____
(Phone)

____
(Fax)

FEDERAL DEBARRED LIST CERTIFICATION

Certification Regarding 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; (

(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) (a) “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 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.

(Email address)

(Signature required)

(Print name)

(Print title)

(Address)

(Phone)

(Fax)

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.

____
(Email address)

____
(Address)

____
(Signature required)

____
(Phone)

____
(Print name)

____
(Fax)

____
(Print title)

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

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

Solid Waste

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

Water Waste

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

Packaging

1. What is your firm's plan to minimize packaging and/or describe your firm's packaging "Take Back" program?

2. What kind of reusable, recyclable, and/or compostable packaging materials does your firm use?
3. What does your firm do to encourage/require your suppliers to minimize packaging and/or use reusable, recyclable, or compostable packaging materials?

Sustainability Practices

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

Community

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

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

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

Water Waste

EPA information about conserving water:

- http://water.epa.gov/polwaste/nps/chap3.cfm

Packaging

- http://sustainablepackaging.org/uploads/Documents/Definition%20of%20Sustainable%20Packaging.pdf

Sustainability Practices

Ideas for alternative transportation programs:

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

Ecologo cleaning and janitorial products:

- http://www.ecologo.org/en/certifiedgreenproducts/category.asp?category_id=21

SECTION XIV – SECURITY REVIEW (FOR REFERENCE ONLY)

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.

□	**Medium**	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. However the vendor has not provided evidence of compliance with the ISO language.
□	**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

Number of Records	ex: 5000	Are direct services performed in the US?	ex: 5000
Estimated Yearly Addition	ex: 500	Is data stored in the US?	Yes/No
Are records purged?	Yes/No	Are data or systems accessible outside the US?	Yes/No

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

apply.) Regulated Data

□ PCI regulated (credit card data)

□ FERPA regulated (student data)

□ GDPR regulated (European Union user data)

□ HIPAA regulated (health data)

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

☐ Other Regulated (CJIS, COPPA, GLBA, etc.)

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.
□	**High**	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).
□	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
□	**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.
□	**High**	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).
□	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
□	**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 vulnerability 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.

SECTION XIV – SECURITY ARCHITECTURE DIAGRAM (REFERENCE DOCUMENT #2)

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

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

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

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

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

You are now ready to start making your drawing.

- Choose a symbol to represent the endpoints. Typically this is a box, but it could be something else. Draw a box (if that's your choice) for each endpoint. Again, that would be one box to represent all the users who share a single role, and another box for each server (or group of identical servers). If different users connect to different servers, that would be a distinct endpoint. Don't forget the users! The system can't work without them.

- Label endpoints that are permanent (e.g. servers) with their IP address and/or Fully Qualified DNS hostname*. Users, of course, come and go all the time, and their IP address or name doesn't matter.

- Choose a symbol to represent the connections. Typically this is a line, but it could be something else. Draw a line (or whatever) from each endpoint to each other endpoint with which it communicates.

- Choose a symbol to identify which end of the connection is the client and which end is the server. Remember that the server is passively listening on a port for requests, and the client is initiating those requests. You could represent this, for example, by an arrowhead on the server end of the line, indicating that the client sends a connection request to the server.

- Near the server end of the connection, identify the port number on which the server is listening.

- Indicate the communication protocol used by the connection. For example, a web site may use the http or https protocol. Even for public sites, https is preferred.

- Describe, on the diagram or elsewhere, what type of data is flowing along each connection. Is it confidential? Regulated? If the data is sensitive, describe how it is protected in transit. For example, is it encrypted? Using what type of encryption? Describe any controls to limit who or what can connect and fetch the information.

- If there is confidential or sensitive data, describe how it is protected at each endpoint of the connection. Is it encrypted at rest? If so, how? Is the endpoint protected by a firewall? If so, what does the firewall block or allow? Is the data viewed but not stored (e.g. by a client) so that secure storage is a non-issue?

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

Summary

So for each server (anything that accepts connections) you should have:

- Fully Qualified DNS name and/or IP address

- Description of what it is or what it does (web server? database?)

For each connection you should have:

- Port number where theserver is listening

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

Additional Info

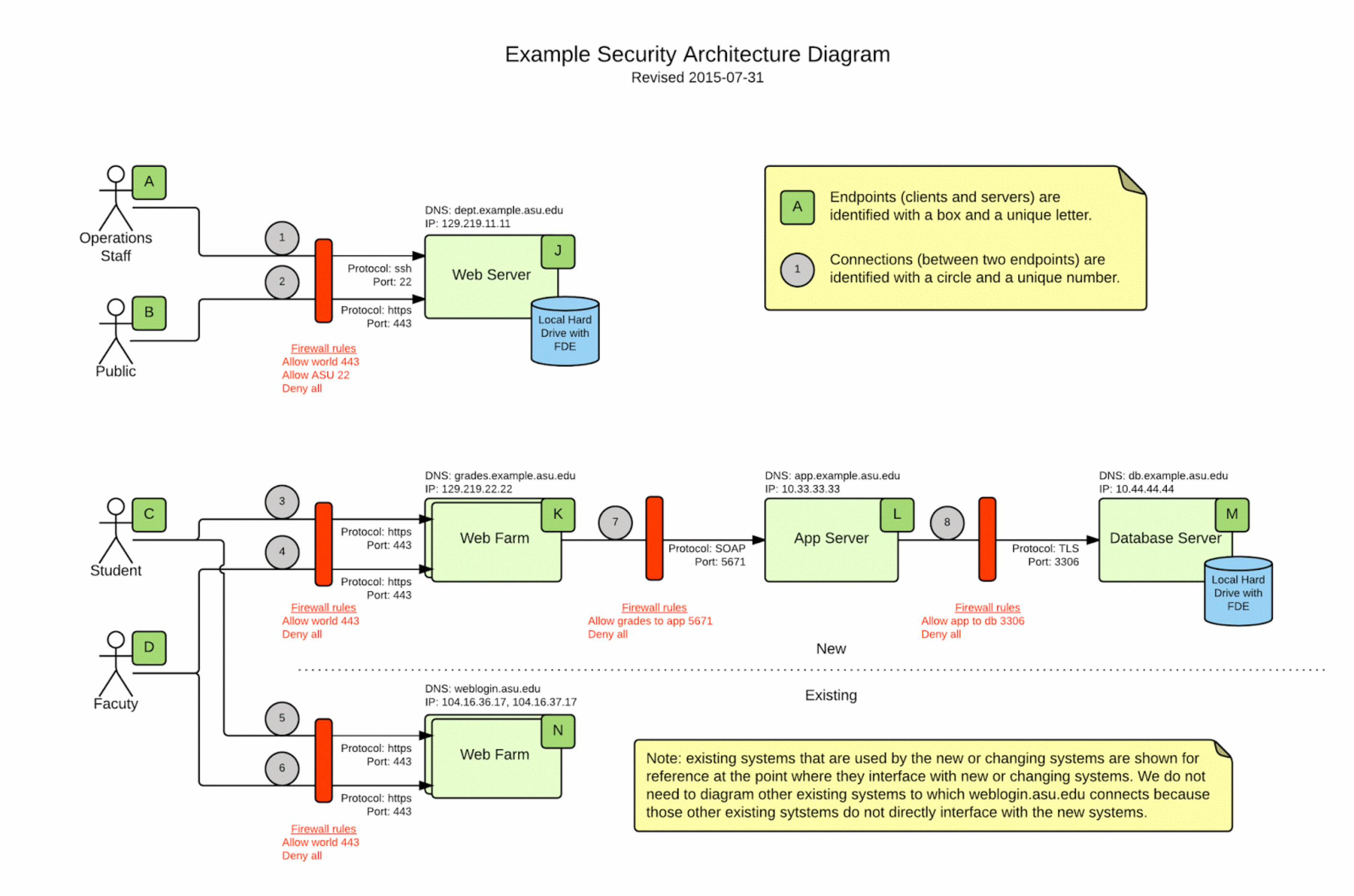
It may also help to distinguish existing endpoints, to which you will merely connect, from new endpoints that will be created as part of your project.

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

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

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

EXAMPLES:

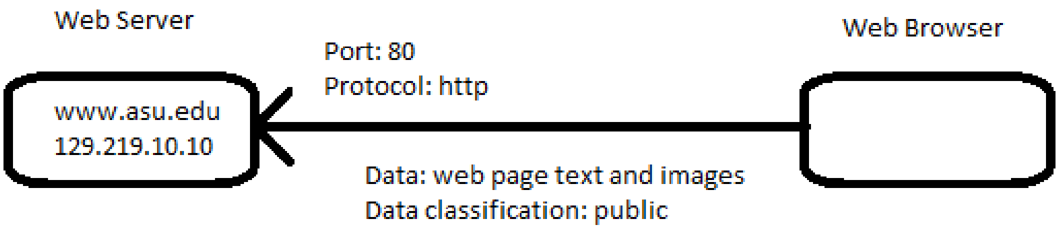


Endpoints (clients and servers) are identified with a box and a unique letter.

Connections (between two endpoints) are identified with a circle and a unique number.

Note: existing systems that are used by the new or changing systems are shown for reference at the point where they interface with new or changing systems. We do not need to diagram other existing systems to which weblogin.asu.edu connects because those other existing sytstems do not directly interface with the new systems.

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



Arizona State University

APPENDIX 1 – RFP CHECKLIST/COVER PAGE

This Appendix 1 is required at the front of your proposal and completed in its entirety. The following documents are required for this proposal (please mark off each document to acknowledge that you have submitted the document in the proper order and format):

□	**Section 1**	**RFP Checklist/Cover Page, Mandatory Certifications, & Supplier Sustainability Questionnaire.**
□	**Section 2**	**Proposer Qualifications, Section VII (Maximum 20 pages not including resumes, CVs, and/or Organizational charts. Do not include Financial Statements – see Section 6 below).**
□	**Section 3**	**Response to the Specifications/Scope of Work, Section V.**
□	**Section 4**	**Response to Price Schedule, Section IX.**
□	**Section 5**	**Exceptions to Terms and Conditions, Section XII**
□	**Section 6**	**Financial Statements**
□	**Section 7**	**Confidential/Proprietary Justification Letter with Sealed documents, if applicable. Section IV, page 9, item 9.**

In addition, the proposer must provide their review and acknowledgement of the following documents provided in this RFP (please mark off each document to acknowledge that you have reviewed the below documents in the RFP)

□	**RFP 342006 (PDF Document)**
□	**All RFP Addendums (PDF Document)**

After carefully reviewing all the terms and conditions, the authorized undersigned agrees to furnish such goods/services in accordance with the specifications/scope of work.

Firm (CO.) Name	By (Signature)	Title
Date	**Email Address**	**Phone #**