



April 10, 2019

**REQUEST FOR PROPOSAL
CONTACT CENTER SOLUTION
RFP 341905
DUE: 3:00 P.M., MST, 05/16/19**

Time and Date of Pre-Proposal Conference	3:00 P.M., MST, 04/23/19
Deadline for Inquiries	3:00 P.M., MST, 05/06/19
Time and Date Set for Closing	3:00 P.M., MST, 05/16/19

TABLE OF CONTENTS

<u>TITLE</u>	<u>PAGE</u>
SECTION I – REQUEST FOR PROPOSAL	3
SECTION II – PURPOSE OF THE RFP.....	4
SECTION III – PRE-PROPOSAL CONFERENCE.....	6
SECTION IV – INSTRUCTIONS TO PROPOSERS.....	7
SECTION V – SPECIFICATIONS/SCOPE OF WORK	12
SECTION VI – GREEN PURCHASING REQUIREMENTS/SPECIFICATIONS	21
SECTION VII – PROPOSER QUALIFICATIONS	22
SECTION VIII – EVALUATION CRITERIA.....	24
SECTION IX – PRICING SCHEDULE	25
PLEASE SEE EXHIBIT C - PRICING SCHEDULE ATTACHED.....	25
SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS	26
SECTION XI – PROPOSER INQUIRY FORM	27
SECTION XII – AGREEMENT - TERMS & CONDITIONS	28
SECTION XIII – MANDATORY CERTIFICATIONS.....	51
SECTION XIV - SECURITY REVIEW	60
SECTION XIV – SECURITY ARCHITECTURE DIAGRAM (REFERENCE DOCUMENT #2).....	79
APPENDIX 1 - RFP CHECKLIST/COVER PAGE	83

SECTION I – REQUEST FOR PROPOSAL

RFP 341905

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Contact Center Solution**.

Proposals are to be addressed and delivered to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, (located on the east side of Rural Road between Apache Boulevard and Broadway Road) Tempe, Arizona 85281 **on or before 3:00 P.M., MST, May 16, 2019**. **No proposal will be accepted after this time. PROPOSALS MUST BE IN A MARKED SEALED CONTAINER** (i.e., envelope, box):

Name of Proposer
Title of Proposal
RFP Number
Buyer's Name (Lorenzo Espinoza)
Date and Time Proposal is Due

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

A representative of Purchasing and Business Services will announce publicly the names of those firms or individuals submitting proposals. No other public disclosure will be made until after award of the contract.

Arizona State University's Overnight Delivery (FedEx, Airborne, and UPS) address is:
Purchasing and Business Services
University Services Building
Arizona State University
1551 S. Rural Rd
Tempe, AZ 85281

Arizona State University's U.S. Postal Service Mail address is:
Purchasing and Business Services
Arizona State University
P.O. Box 875212
Tempe, AZ 85287-5212

ARIZONA STATE UNIVERSITY

Lorenzo Espinoza, Senior Buyer
LE/AP

SECTION II – PURPOSE OF THE RFP

1. INTENT

The Arizona Board of Regents (ABOR), on behalf of Arizona State University (ASU), is seeking proposals from firms with extensive experience in higher education to furnish the University with a comprehensive contact center solution (CCS) as described in the scope of work. ASU is seeking a cloud hosted omni-channel Contact Center Solution (CCS) to provide better insights and data for the university to use to improve services, processes and get an “in the moment” view of sentiment across the university community. ASU expects a solution that has the opportunity to collect detailed data at every possible point of contact between our ASU community and the ASU Contact Center, be that by phone call, chat, social media interactions and communication platforms yet to come. ASU imagines the power of leveraging this data for its students and customers, and the ability to have a complete word for word record of an interaction to then analyze. The power of this can be as simple as an executive dashboard that shows the live sentiment broken down by key university service areas to being able to provide deeper insights into friction points between our students and the services they count on for success in their life long journey of learning.

The power of the data that ASU envisions can go even deeper, becoming the intelligence to feed advanced machine learning technologies and drive artificial intelligence systems such as chatbots (a.k.a. natural language auto-response system) and voice enabled assistants. ASU has a rare opportunity now to invest in a system that can be the foundational intelligence gathering system that feeds and drives other innovative solutions to enhance the experience of service and student engagement across the institution. ASU wants this to be the contact center solution that all departments will want to leverage and take advantage of, and to be the foundation of the intelligent university, that uses actual “in the moment” student voice data to launch ASU into the next decade of innovation and to jump the curve in the collection and use of data to get there.

This will be an investment in the future of Arizona State University and has the potential to be the richest source of direct student experience data.

2. BACKGROUND INFORMATION

ASU’s University Technology Office (UTO) provides the highest quality technology-based services and systems, in a cost-effective manner, to support the University’s mission and goals as they apply to student learning, academic research and public service. In 2014, ASU implemented a Contact Center Solution. Since the implementation of the present solution, technology has changed, our ASU family’s expectations have grown and new opportunities in

data collection, analytics and artificial intelligence have surfaced. We are at a perfect intersection of time and technology advancements that we could turn the Contact Center into a complete ASU Experience Center. The solution we implement today will not just be the front door for all major ASU services but also the heart of data collection for the deepest understanding of our students, process friction points and overall ASU community sentiment.

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 three (3) year(s) with the possibility of two (2) successive one (1) year renewals, for a total term not to exceed five (5) years. The contract will be available for use by other University departments during this term.

The University may consider alternative contract term periods if it is deemed advantageous to do so. If alternative contract terms are proposed, please specify an alternate in the space provided. Note: Alternative terms cannot be in lieu of the term stated above.

SECTION III – PRE-PROPOSAL CONFERENCE

A pre-proposal conference will be held online on Thursday, April 23, 2019 at 3:00P.M. via video conference.

A pre-proposal conference will be held online on Thursday, April 23, 2019 at 3:00P.M. The purpose of this conference will be to clarify the contents of this Request for Proposal in order to prevent any misunderstanding of the University's intention and desires. Any doubt as to the requirements of this solicitation, or any apparent omission or discrepancy should be presented to the University representative at this conference. The University representative will then determine the appropriate action. If necessary, the University representative will issue a written amendment to this Request for Proposal. Oral statements or instructions shall not constitute an amendment to this Request for Proposal.

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

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

1. **Register by 5:00 p.m. on Monday, April 22, 2019**, for the event by sending an email of participants to include to Lorenzo.Espinoza@asu.edu. Include the following information:
 - a. First and Last Name
 - b. Company
 - c. Title
 - d. Email address
 - e. Phone Number
2. On the day of the conference registered users will be provided a passcode to enter the virtual room.

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

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

SECTION IV – INSTRUCTIONS TO PROPOSERS

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

Name of Proposer

Title of Proposal

RFP Number

Buyer's Name (Lorenzo Espinoza)

Date and Time Proposal is Due

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

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

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

3. Proposer should use recycled paper and double-sided copying for the production of all printed and photocopied proposal documents. Furthermore, the documents should be clearly marked to indicate that they are printed on recycled content (minimum 30% post-consumer waste paper).
4. You may withdraw your proposal at any time prior to the time and date set for closing.
5. No department, school, or office at the University has the authority to solicit or receive official proposals other than Purchasing and Business Services. All solicitations are performed under the direct supervision of the Chief Procurement Officer and in complete accordance with University policies and procedures.
6. The University reserves the right to conduct discussions with proposers, and to accept revisions of proposals, and to negotiate price changes. During this discussion period, the University will not disclose any information derived from proposals submitted, or from discussions with other proposers. Once a contract is executed, the solicitation file, and the proposals contained therein, are in the public record and will be disclosed upon request.
7. Proposers submitting proposals which meet the selection criteria and which are deemed to be the most advantageous to the University may be requested to give an oral presentation to a selection committee. Purchasing and Business Services will do the scheduling of these oral presentations.

8. The award shall be made to the responsible proposer whose proposal is determined to be the most advantageous to the University based on the evaluation factors set forth in this solicitation. Price, although a consideration, will not be the sole determining factor.
9. If you are submitting any information you consider to be proprietary, you must place it in a separate envelope and mark it "Proprietary Information". If the Chief Procurement Officer concurs, this information will not be considered public information. The Chief Procurement Officer is the final authority as to the extent of material, which is considered proprietary or confidential. Pricing information cannot be considered proprietary.
10. The University is committed to the development of Small Business and Small Disadvantaged Business ("SB & SDB") suppliers. If subcontracting (Tier 2 and higher) is necessary, proposer (Tier 1) will make every effort to use SB & SDB in the performance of any contract resulting from this proposal. A report may be required at each annual anniversary date and at the completion of the contract indicating the extent of SB & SDB participation. **A description of the proposers expected efforts to solicit SB & SDB participation should be enclosed with your proposal.**
11. Your proposal should be submitted in the format shown in Section X. Proposals in any other format will be considered informal and may be rejected. Conditional proposals will not be considered. An individual authorized to extend a formal proposal must sign all proposals. Proposals that are not signed may be rejected.
12. The University reserves the right to reject any or all proposals or any part thereof, or to accept any proposal, or any part thereof, or to withhold the award and to waive or decline to waive irregularities in any proposal when it determines that it is in its best interest to do so. The University also reserves the right to hold all proposals for a period of **one hundred twenty (120) days** after the opening date and the right to accept a proposal not withdrawn before the scheduled proposal opening date.
13. **EXCEPTIONS:** The Arizona State University contract terms and conditions are included in this Request for Proposal in Section XII. These terms and conditions will be incorporated into the contract between the University and the successful proposer. **Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed nonresponsive and may be rejected.** All exceptions must be submitted with justification and alternate language, and **MUST** be submitted with the proposal. In no event is a Proposer to submit its own standard contract terms and conditions as a response to this RFP.
14. Unless specifically stated to the contrary, any manufacturer's names, trade names, brand names or catalog numbers used in the specifications of this Request for Proposal are for the purpose of describing and/or establishing the quality, design and performance required. Any such reference is not intended to limit or restrict an offer by any proposer and is included in order to advise the potential proposer of the requirements for the University. Any offer, which proposes like quality, design or performance, will be considered.
15. Days: Calendar days
 May: Indicates something that is not mandatory but permissible/ desirable.
 Shall, Must, Will: Indicates mandatory requirement. Failure to meet these mandatory requirements will result in rejection of your proposal as non-responsive.

Should: Indicates something that is recommended but not mandatory. If the proposer fails to provide recommended information, the University may, at its sole option, ask the proposer to provide the information or evaluate the proposal without the information.

16. Any person, firm, corporation or association submitting a proposal shall be deemed to have read and understood all the terms, conditions and requirements in the specifications/scope of work.
17. All proposals and accompanying documentation will become the property of the University at the time the proposals are opened. **It will be the proposer's responsibility to request that samples be returned to the proposer and provide a method for doing so at the expense of the proposer.** If a request is not received and a method of return is not provided, all samples shall become the property of the University 45 days from the date of the award.
18. All required performance and payment bonds shall be held by the University in a secure location until the performance of the contract and the payment of all obligations rising there under have been 100% fulfilled. Upon completion of the project and all obligations being fulfilled, it shall be the proposer's responsibility to request the surety bonding company to submit to the University the necessary documents to approve the release of the bonds. Until such time the bonds shall remain in full force and effect.
19. The University of Arizona, Northern Arizona University, and Arizona State University are all state universities governed by the Arizona Board of Regents. **Unless reasonable objection is made in writing as part of your proposal to this Request for Proposal, the Board or either of the other two Universities may purchase goods and/or services from any contract resulting from this Request for Proposal.**
20. Arizona State University is a member of various co-operative organizations, in accordance with A.R.S. Sections 11-952 and 41-2632. Under these Cooperative Purchasing Agreements, the University may share and distribute a contract resulting from a solicitation. In the absence of a statement to the contrary, the University will assume that you do wish to grant access to any contract that may result from this Request for Proposal.
21. Administrative Fee: Awarded Suppliers shall pay ASU an Administrative Fee in the amount of 1 percent of the gross funds received by the Supplier from any of the Arizona Entities or any other similar entity in any other state. This fee will apply only to contracts entered into after the effective date of the signed contract. This fee will apply to any and all products and services sold by the Supplier that reference the signed contract as the supporting documentation to meet competitive bidding requirements. The Administrative Fee will be calculated based on all sales transacted under the contract, minus all taxes and any returns or credits. The supplier will submit the Administrative Fee, along with a quarterly usage report documenting all contract sales, to the ASU Chief Procurement Office within thirty (30) days following the end of each calendar quarter. Each quarterly report at a minimum, shall disclose all purchased goods and services, prices paid, and quantity, by individual purchasing agency, for all sales within the calendar quarter just ended. The Supplier will upload to and make continuously available in the Central Repository the quarterly usage report.
22. All formal inquiries or requests for significant or material clarification or interpretation, or notification to the University of errors or omissions relating to this Request for Proposal must be directed, in writing, to:

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

Tel: 480-296-3134
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 answer informal questions orally. The University makes no warranty of any kind as to the correctness of any oral answers and uses this process solely to provide minor clarifications rapidly. Oral statements or instructions shall not constitute an amendment to this Request for Proposal. Proposers shall not rely on any verbal responses from the University.

23. The University shall not reimburse any proposer the cost of responding to a Request for Proposal.
24. In accordance with an executive order titled "Air Pollution Emergency Proclamation" modified by the Governor of Arizona on July 16, 1996, the University formally requests that all products used in the performance of any contract that results from this Request for Proposal be of low- or no-content of reactive organic compounds, to the maximum extent possible.
25. Arizona requires that the University purchase ENERGY STAR® products or those certified by the Federal Energy Management Program as energy efficient in all categories available. If this Request for Proposal is for a product in a category for which ENERGY STAR® or certified products are available, please submit evidence of the ENERGY STAR® status or certification for the products you are bidding. Please note that if you fail to submit this information but a competitor does, the University will select your competitor's product as meeting specifications and deem your product as not meeting specifications. See A.R.S. §34-451.
26. The University requires that all desktop computers, notebooks, and monitors purchased must meet Electronic Product Environmental Assessment Tool (EPEAT) Gold status as contained in the IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products. The registration criteria and a list of all registered equipment are at <http://www.epeat.net/about-epeat/> on the Web.
27. To the extent applicable to any contract resulting from this Request for Proposal, the proposer shall comply with the Standards for Privacy of Individually Identifiable Information under the Health Insurance Portability and Accountability Act of 1996 contained in 45 CFR Parts 160 and 164 (the "HIPAA Privacy Standards") as of the effective date of the HIPAA Privacy Standards on April 14, 2003 or as later determined. Proposer will use all security and privacy safeguards necessary to protect Protected Health Information (PHI), as defined by HIPAA, and shall immediately report to University all improper use or disclosure of PHI of which it becomes aware. Proposer agrees to ensure that its agents and subcontractors agree to and abide by these

requirements. **Proposer agrees to indemnify the State of Arizona, its departments, agencies, boards, commissions, universities and its officers, officials, agents, and employees against all harm or damage caused or contributed to by proposer's breach of its obligations under this paragraph.**

- 28.** The University believes that it can best maintain its reputation for treating suppliers in a fair, honest, and consistent manner by conducting solicitations in good faith and by granting competitors an equal opportunity to win an award. If you feel that we have fallen short of these goals, you may submit a protest pursuant to the Arizona Board of Regents procurement procedures, section 3-809,

Protests should be directed to:

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

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

SECTION V – SPECIFICATIONS/SCOPE OF WORK

The top level requirements for this RFP are as follows:

(Note: these requirements are laced throughout the Scope of Work and will be identified by an *italics underlined* within the document.)

1. *100% cloud-based solution that requires no on premises hardware.*
2. *Provide Interactive Voice Response (IVR), Automatic Call Distributor (ACD) and Workforce Optimization (WFO) capabilities.*
3. *ASU requires the CCS to be fully redundant.*
4. *The CCS platform, its accompanying applications, training, etc., as outlined in the contract negotiations and implementation schedule, shall be fully active and live as of July 1, 2020.*
5. *Due to the nature of University business, all implementation costs associated with the build, support and integration of the CCS platform will be paid upon successful go-live on July 1, 2020.*
6. *The CCS platform must provide live dashboarding capability.*
7. *The CCS must provide deep and insightful data collected from every interaction (voice to text, chat/SMS transcriptions, social media transcriptions related only to ASU, mobile application interactions, etc.)*
8. *The ability to run a “what-if” analysis using past data to predict the potential impacts.*
9. *ASU must have predictive analytics to be able to interpret data through the lens of patterns and trends, and use those findings to forecast future performance.*
10. *ASU must be able to store all data in the ASU Data Lake within Amazon Web Services (AWS).*
11. *The CCS platform must meet ASU security standards (firewall, port configurations, data encryption, etc.).*
12. *The CCS platform must integrate with all modern forms of security implementations, including end-to-end encryption, two-factor authentication, single sign-on, and secure integrations to other databases (Salesforce, ServiceNow, Peoplesoft, etc.).*
13. *The CCS must be able to have enhanced self-service options such as voice recognition as well as Dual-tone multi-frequency (DTMF) (press 1 for..), real time queue “callers ahead” information, robust Artificial Intelligence (AI)/chatbot functionality, and omni-channel integration with email, web callback scheduling, chat, text, social media, video chat, etc.*
14. *The CCS platform must be designed to incorporate new AI technologies*
15. *The CCS platform must have the ability to integrate with ASU’s mobile app and be able to verify and authenticate the users security credentials and be able to route the user based on their selected or spoken support needed.*
16. *ASU requires the CCS to be flexible with the ability to integrate with its 4 major enterprise systems (Salesforce, ServiceNow, Peoplesoft and Workday Financial)*
17. *ASU requires a workforce management (WFM) application and its associated tools.*
18. *ASU requires quality assurance tools including the ability to record all interactions, store a transcript of those recordings into a Salesforce case and capture/record all desktop support screens with synchronization to the call recording.*
19. *The CCS platform must have a mobile application that will allow management to monitor support volumes, perform real-time Quality Assurance (QA) monitoring and modify routing skills for support staff.*

Key objectives of this CCS initiative

I. Omni-Channel Contact Center Solution

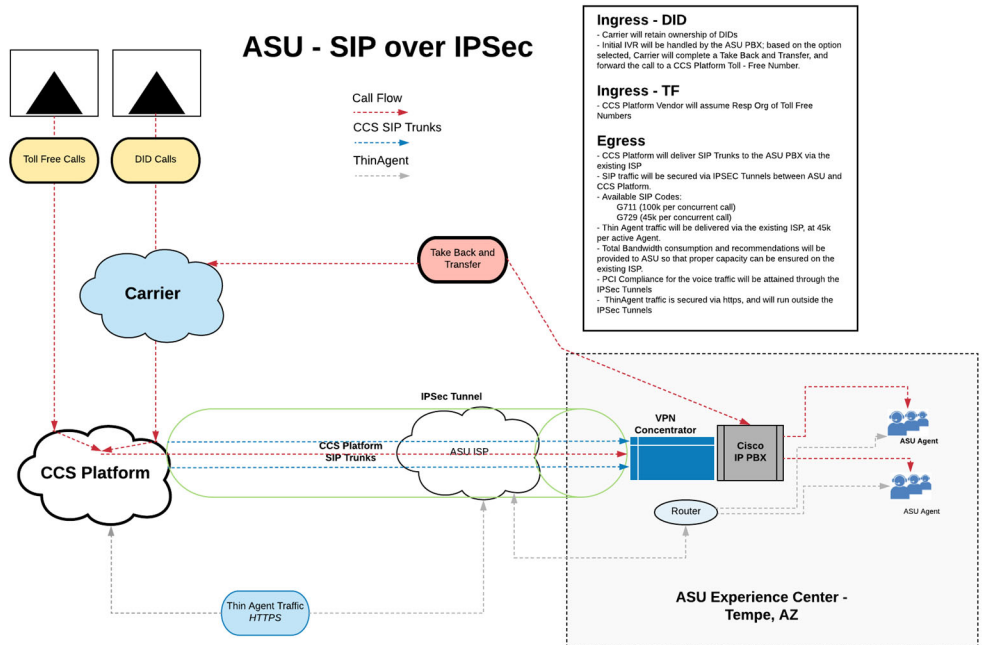
ASU currently utilizes a cloud-based CCS to operate its Experience Center on a 24x7x365 timeframe. Additionally, there are some smaller support groups across its academic campuses that do not utilize the current cloud-based Contact Center Solution. Currently, the ASU CCS is managing voice calls only. We need a CCS that can incorporate and manage all channels of communication (Chat, SMS, email, Social Media, Mobile Applications, Video (Zoom), etc.) and meet the expanded contact center support demands and enhance our data gathering for more sophisticated support tools and intelligent reports.

ASU's current enrollment is over 111,000 students with support from 28,000 faculty, staff and student employees. A significant portion of the student enrollment includes approximately 37,000 online students. ASU's online program, currently utilizing the same Contact Center Enterprise Solution, is looking for a CCS solution that will enhance our student coaching and recruitment capabilities and provide intelligent reporting that will lead ASU to have better retention rates, influence contact strategies and improve the overall student experience.

II. System Architecture (*Stability, Expansion/Capacity, Fault Tolerance & Disaster Recovery*)

The CCS must be 100% cloud-based solution that requires no on premises hardware and have dependable service under heavy usage applications. It must provide IVR, ACD and WFO capabilities. Performance standards must equal or exceed the current level (99.999%). The CCS must offer safeguards to allow call processing during major component failures and commercial power interruptions. Fault tolerance and failover safe guards must be seamless to ASU. The CCS is

expected to be a sophisticated omni-channel routing, comprehensive contact management integration with Salesforce and integration with ServiceNow for Information Technology Infrastructure Library (ITIL) processes capable of providing support to the ASU community (students and employees) located across multiple locations in the ASU infrastructure. The CCS provider must provide a diagram of their system architecture. The adjacent image is our current architecture diagram. Please note that ASU owns all their direct inward dialing (DiD) numbers and our current CCS provider owns all the toll free numbers (TFN).



Looking to future growth, ASU must have a CCS platform capable of scaling in real time to include employees who have not previously been associated with any call center group in the past. ASU experiences huge spikes in support volume during the start of each semester. ASU's current CCS provides the ability to increase ports with a simple request to the vendor. ASU needs infinite capacity to add agents on the fly, unlimited queues, infinite prompts, and infinite number of skills across their CCS platform. In the event of an emergency the ability to scale quickly will dictate a need to immediately increase agent capacity. During an emergency crisis, the CCS will need to use employees not previously associated with the contact center, such as non-IT staff, outside vendor-contracted staff, clerical staff and management. ASU CCS must be capable of making modifications, such as extension number changes, station feature revisions and database updates with a minimum of dependence on outside support.

Due to the critical nature of our contact center and its support expectations, the CCS must be reliable and stable. ASU requires the CCS and its cloud-based hosted provider to detect and diagnose system failures quickly and efficiently and handle repairs expeditiously. The CCS must provide a system health type report that is monitoring network connectivity, fault isolation (trunks and lines) and provide a communication process for notification of service failures and their estimated time for resolution.

ASU requires the CCS to be fully redundant. ASU understands that power failures happen. However, due to the high level of expected uptime (99.999%) that our contact center operates, ASU CCS must have safeguards that allow continuous omni-channel processing in the event of a power outage or system wide network outage at the host provider solution primary location. The CCS platform vendor will need to provide a DRP for their CCS platform solution.

Due to the operational nature of a higher education institution, ASU has limited windows of opportunity for maintenance updates. ASU cannot afford for maintenance updates to impact the academic mission of the university. The CCS must readily accept software updates, hardware expansions and reconfigurations without loss of service. These scheduled maintenance updates must be performed in a minimal amount of time, they must occur in timeframes that provide minimum impact to the Experience Center's hours of operation which are 24X7X365 and they should occur at the lowest possible cost.

ASU contracts its network infrastructure and its telephony infrastructure to an outside contractor. ASU needs the CCS to be modular. The CCS platform must interface with the public switched telephone network (PSTN), private network facilities, other corporate cloud-based hosted systems (Salesforce, ServiceNow, Peoplesoft, etc.) and wide area networks and the Internet with minimal engineering activity and expense. The CCS must provide documentation on new features and capabilities as it enhances the cloud-based hosted system.

Finally, the current CCS requires an on-premise server for handling screen capture and recording of all Experience Center support staff active CCS desktops. The screen capture and recording files are automatically synced to all voice recordings related to each individual support session. ASU requires a CCS that would not require an on-premise server but be 100% cloud-based.

III. Pre-Implementation, Training and Technical Support

In 2014 ASU implemented a CCS in sixty days. The initial 60-day implementation did not include a survey tool, workforce management (WFM) tool, quality analytics tool, outbound dialer tool, or the specialized automated IVR feature developed with API connection to Salesforce configured as a self-service financial aid auto-response tool. The 60 day implementation schedule did include a CCS platform consultation with ASU stakeholders, an integration with the CCS platform to the Salesforce Customer-Relationship Management (CRM) for phone identification that would determine the caller's relationship with ASU (Student or Employee) and a push of the Salesforce Bio data to a Visualforce interface pop for students and a ServiceNow pop for employees.

A new CCS platform provider will be expected to perform the same initial Salesforce interactions and include all the added features (WFM, Surveys, QA, Outbound Dialed and Self Service Auto-Response) as previously mentioned across all business units.

The CCS platform, its accompanying applications, training, etc., as outlined in the contract negotiations and implementation schedule, shall be fully active and live as of July 1, 2020. Currently, ASU has a working CCS platform including WFM and QA. This current active CCS platform will provide a prospective vendor a 6-9 month pre-implementation phase/time frame. The pre-implementation phase should be used to scope and configure a fully functional CCS platform with minimal impact to ASU operations. The awarded vendor must use this 6-9 month period to implement the following (this list may not be inclusive of all required integrations needed for a successful launch):

- Volume load-testing on the network infrastructure
- Security integrations within the ASU network infrastructure using encrypted connections.
- Integration with ASU single-sign-on (SSO).
- ACD Automated Survey Tool for Customer Response after support call ends.
- Quality Analytic Dashboards detailing call metrics hourly, daily, monthly and annually in real time.
- Nightly data dumps of all ASU data to the ASU data warehouse.
- Integration between the CCS platform and the Salesforce (CRM) DB for phone identification (ANI) that would capture the caller's bio data as an ASU student or employee and then do the following:
 - The CCS platform will utilize the Salesforce Bio data to create and pop a Visualforce page for creating Salesforce case.
 - The CCS platform will utilize the Salesforce Bio data to create and pop a ServiceNow ticket for tracking employee issues.
- ASU mobile app development for pre-authenticated users, including skill-based routing.
- CCS platform can securely authenticate callers using voice and facial recognition algorithms.
- Salesforce integration with the CCS platform including but not limited to, Visualforce, query for skills-based routing, and LiveAgent.
- ACD/IVR development including the Financial aid (FA) self-service tool using DTMF input.

- Quality assurance (QA) tool development with specialized QA forms and desktop screen recording/capture tool
- Quality assurance call monitoring on all recorded calls and are synchronized to all support staff desktop screen recordings.
- Workforce management (WFM) tool development
- Predictive outbound dialer configurations for campaigns and all specialized development work for the ASU online program

Please note, most of the specialized development work and integrations are utilizing the ASU Peoplesoft and Salesforce enterprise systems.

Due to the nature of University business, all implementation costs associated with the build, support, transition and integration of the CCS platform will be paid after the successful go-live on July 1, 2020.

The Experience Center requires a dedicated technical support liaison from the CCS provider that can be reached out to with any questions or concerns. Weekly teleconference meetings are expected to be held to discuss open technical support cases, bring up new issues that are being experienced, or discuss how to proceed with growing business needs and business expenses. Along with this, the Experience Center requires access to a Professional Services help line that can assist with any real-time technical issues that may occur.

The Experience Center is a 24/7/365 operation and as such, needs to have access to 24/7/365 technical support for their CCS system. The prospective CCS provider needs to allocate a dedicated specialist to be available for questions and to assist in monitoring and expediting technical cases that are submitted for resolution. The CCS provider would also need to provide 24/7/365 support for any technical issues that may occur.

The ASU University Technology Office (UTO) Instructional Design and Training team will be responsible for training existing and new Contact Center employees on the prospective system. Trainers need to be trained on the prospective system by the provider. Provider is expected to provide train-the-trainer sessions. The trainers will be provided with job aid collateral as reference material as they pass on the new information to the new and existing employees. The trainers also need to be able to ask follow-up with questions post-training; a designated point-of-contact is preferred.

The system functionality needs to enable new hires to take practice calls in a sandbox or test environment prior to exiting training. The sandbox is expected to mirror the live environment exactly. Other required capabilities include live monitoring and live screen capture.

IV. Intelligent Data Gathering, Reporting and Data Security

ASU is looking to enhance its ability to maintain, develop and increase its critical business intelligence gathering by adding features to its current CCS business processes. ASU expects the CCS platform to provide live dashboarding capability.

The CCS must provide deep and insightful data collected from every interaction (voice to text, chat/SMS transcriptions, social media transcriptions related only to ASU, mobile application interactions, etc.) for more enhanced/detailed reports and business strategy.

1. ASU must have the ability to view performance metrics within the ASU Experience Center and offer similar capabilities to participating departments. The ability to find hidden qualitative trends in data across all services within the data collected. ASU seeks to develop “what-if” analysis to better determine how a future decision will affect our current business and future business needs. The ability to run a “what-if” analysis using past data to predict the potential impacts. Tools for “what-if” analyses that give ASU an objective view of the risks and rewards involved in each potential decision, and allow ASU to plan better for the future.
2. ASU requires its dashboards to allow ASU’s organizational leadership a real-time overview of our business in the form of graphs, charts, summaries and other informational reports; the ability to allow ASU’s executives to make smarter, faster and better decisions. ASU needs to allow its executives and stakeholders the ability to condense and consume massive amounts of collected data into a wide variety

of possible views. The ability to provide ASU executives and stakeholders a detailed summary of the daily events and providing them with the information they need to make critical decisions. ASU expects to have the ability to provide ad-hoc reports for non-technical end-users that generate their own reports on the fly. These reports will allow ASU users to pick and choose the elements that they wish to be included in their ad-hoc report, emphasizing only those aspects that are relevant to their query. The proposed solution should allow ASU to take advantage of features like statistical analysis and regression to identify trends, anomalies and outliers in the data using provided tools from the proposed solution in addition to in-house tools by sifting through the raw data internally.

3. ASU requires geospatial mapping and using location intelligence that can utilize our collected information and transform it into graphical and cartographic representations, simplifying our geographical data. Providing at a glance the ability to judge which region or regions are performing better than others and which ones need particular attention.
4. ASU requires an open integration solution that would allow smart BI platforms to be able to access not only ASU organizational data from the CCS, but information from chat, email, social media, websites and more. ASU must have predictive analytics to be able to interpret data through the lens of patterns and trends, and use those findings to forecast future performance.
5. ASU must be able to store data in the ASU Data Lake within AWS. In an effort to enhance intelligent data reporting, ASU needs to have data stored in a way that will allow complex data mining. By enhanced data mining, ASU will increase its ability to explore and analyze large data sets.

ASU requires that effective security measures are in place to protect sensitive information, including personally identifiable information, in all its systems and seeks to provide more exhaustive personal information protection for ASU databases including but not limited to Oracle, Sybase, MySQL, MS SQL, AWS Redshift, S3, Aurora, and flat file storage including but not limited to CIFS, AFS, and NFS. ASU requires the CCS platform to be compliant with Telephone Consumer Protection Act (TCPA) regulations. For more detailed information on ASU's data handling standards read ASU's information policy guide. ASU requires all data related to students to meet Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) standards and regulations.

V. System Security

The CCS platform must meet ASU security standards (firewall, port configurations, data encryption, etc.). It must have role based security, due to our support audience, which will encompass multiple departments and groups across multiple ASU campuses.

ASU affiliated populations have credentials that allow single-sign-on (SSO) to almost all enterprise university services. The main SSO protocol is customized version of Central Authentication Service (CAS), although it is sometimes used in conjunction with Shibboleth for web-based service providers external to ASU (e.g. Salesforce, ServiceNow, etc...). Kerberos is used as the authentication protocol for the CAS service. Active Directory and Active Directory Federation Services (ADFS) accounts are provisioned and used for specific Microsoft services. Unix/Linux Lightweight Directory Access Protocol (LDAP) services are also used for group management and access to web-based and other non-Microsoft systems. Multi-Factor Authentication (MFA) is used for all employees authenticating with CAS or ADFS. Some services also require students to use MFA. With this in mind, our CCS platform must integrate with all modern forms of security implementations, including end-to-end encryption, two-factor authentication, single sign-on, and secure integrations to other databases (Salesforce, ServiceNow, Peoplesoft, etc.).

VI. Automatic Call Distribution (ACD) System (Administration, Desktop, Artificial Intelligence, Case Management, Omni-channel, IVR, Routing and Outbound/Predictive Dialing)

ASU requires the CCS to have enhanced self-service options such as voice recognition as well as DTMF (press 1 for...), real time queue "callers ahead" information, robust AI/chatbot functionality, and omni-channel integration with email, web callback scheduling, chat, text, social media, video chat, etc.

ASU requires the CCS to handle separate departments within ASU to be their own entities for autonomous routing and billing purposes.

Our current ACD system allows us the ability to create/modify/maintain custom scripts to control call flow, routing and custom coding at any given time (control time of day routing - open, closed, holidays, emergencies, meetings, etc.) . It also features a GUI which simplifies the managing/scripting of call routing, messaging, recordings, database integration and querying. Another feature of our current ACD system, vendor provides numerous 800 numbers (TFNs) for ASU to use and associate to any desired departments for skills.

ASU is moving forward with AI, Chatbot and technologies. We require the CCS platform to be designed to incorporate new AI, Chatbot and other future technologies.

In addition to integrating AI technologies into the ASU support environment, ASU is enhancing its mobile app to leverage the capabilities of smart-interactions. We are designing our new mobile-smart-app to verify and authenticate our users before connecting them to our CCS platform for automated chat-bot support or live-agent support and service needs. The CCS platform must have the ability to integrate with ASU's mobile app and be able to verify and authenticate the users security credentials and be able to route the user based on their selected or spoken support needed.

ASU has 4 major enterprise systems (Salesforce, ServiceNow, Peoplesoft and Workday Financial) that it utilizes daily in its overall business operation. ASU requires the CCS to be flexible with the ability to integrate with its 4 major enterprise systems (Salesforce, ServiceNow, Peoplesoft and Workday Financial). Furthermore, the CCS must be flexible such that the various business units utilizing the CCS can create, edit, administer, etc. their own, independent scripts/flows.

There are smaller business units that would like to utilize the proposed CCS system. These units have a slightly different use case from an ACD perspective and will utilize blended calling, heavily favored on outbound dialing, to service students. Currently they use a click-to-dial CTI integration with Salesforce. Some of the ancillary business units have expressed an interest in a dialer solution to achieve efficiency in reaching many students. With that being said, the proposed solution shall integrate with Salesforce to:

- Provide CTI integration
 - Click-to-dial
 - Task creation and field notation on an as needed basis per use case
- Automated dialer list creation
- Automated dialer updates (multi-pass) based on events happening in Salesforce
- Time zone, DNC, opt-out, and other compliance regulation adherence
- Insert updates to Salesforce based on outcome
- Multiple number dialing based on the different numbers found on the contact record

The dialer should also come with administrative tools to allow select users to perform the following items, but not limited to:

- Start and stop campaigns based on service levels and business needs
- Create ad hoc campaigns
- Move agents in and out of campaigns based on business needs
- Manage the number of passes per campaign

VII. Workforce Management (WFM) System

ASU requires a workforce management application and its associated tools. The ASU Experience Center utilizes Workforce Management (WFM) software to effectively manage staff schedules and align staffing resources with forecasted demand. This ensures that we are as lean and efficient as possible while at the same time delivering the highest quality support to the ASU community.

The prospective Workforce Management (WFM) platform must support the following features in order for us to operate efficiently and ensure the right resources are in place to deliver high quality support to the ASU community. The prospective WFM platform must offer the ability to set employee schedules based on skills, schedule breaks, and schedule meetings/training sessions. It must integrate with the associated ACD system. Preferably to the degree that agent statuses in the ACD system are tied to scheduled events in the WFM platform.

It must be cloud-based and support 24/7/365 multi-site call center operations. It must offer the ability for users to generate real-time and historical reporting and forecasting for all captured data points. It must offer the ability to optimize schedules based on current call/chat/email/case arrival patterns. It must offer a real-time adherence dashboard to monitor operations. It ideally offers a time off request management system complete with the ability to forecast impact to service levels. Ideally it should offer automated and manual notifications for events that will impact service levels such as no-call no-shows etc.

In lieu of traditional schedules that are on-premise only, ASU utilizes telecommuting schedules. This remote scheduling allows ASU staff to be more environmentally sustainable, provide a distributed location model to enhance service availability redundancy, and a way to augment staff who are unexpectedly absent. Additionally, ASU needs a CCS capable of handling remote activity is for expedient staffing in the event of an emergency event or increased support volumes during our rush periods at the beginning of each semester startup. In addition, our rush periods require our CCS to be scalable for handling increased support volumes. ASU needs to quickly quantify trunk and line port capacities and quickly increase these capacity bottlenecks when required. ASU request that all interested vendors have a CCS capable of supporting staff to securely login remotely from any telephone type and location. The CCS needs to have flexible accessibility to the hosted provider using mainstream Internet browser applications (Google Chrome, FireFox, etc.) and not Microsoft Internet Explorer (IE).

Lastly, our current CCS platform has a mobile app that provides our management staff with the ability to monitor staff work shifts, skills that they are handling, and perform real-time QA call monitoring, This application is designed to operate on an iPad only. It will be expected to have a CCS platform that had a similar product that was able to be used on all types of mobile devices.

VIII. Quality Assurance (QA) System

ASU requires quality assurance tools including the ability to record all interactions, store a transcript of those recordings into a Salesforce case and capture/record all desktop support screens with synchronization to the call recording. As part of our QA business process, ASU records all caller interactions and captures all screen recordings. We store these voice recordings instantly for 90 days. However, the screen capture recordings are stored on our on-premise server instantly and indefinitely. Leaving our voice recordings disconnected after 90 days to our screen capture recordings. We would like to have a means to store both the voice recordings and screen capture recordings on a centralized storage location and maintain synchronization between the two recordings. Additionally, ASU must add voice transcription to our QA process and store the voice transcription within Salesforce. As discussed previously, ASU is highly motivated to expand the use of our call recordings in order to develop deeper levels of intelligent reporting. This added feature will provide ASU the ability to create and automate support processes around more specific customer trends and identify demographic location of the issues for more specifically designed customer support. Also, these intelligent reports could aid in the development of AI technology (i.e. voice-enabled response system, chatbots, etc.) that could help offload staffing resources during peak volume times.

Currently, ASU management has an iPad application that allows one to do real-time QA monitoring and modify routing skills in real-time as support volumes dictate. The CCS platform must have a mobile application that will allow management to monitor support volumes, perform real-time QA monitoring and modify routing skills for support staff.

The ASU's QA teams' reviews data recordings, chat transcriptions and web to case emails as part of their quality assurance analysis. As we look to enhancements, the ASU QA teams would like to have real-time sentiment analysis of our support staff. Our current QA process reviews at least 4-6 calls per staff, per month. Most of our QA reviews occur on a 24 hour delayed process. The review focuses on incoming phone calls, chats and web-to-case emails and the future vision is to add SMS, text messaging, twitter, and social media. To capture our QA analysis, the QA Coaches utilize a custom developed form to score the staff interactions with our customer. The scorecard is divided into sections, ie. Opening, Problem Solving, Soft Skills and Closing. These sections have subsections associated to them and are scored by the QA coaches; when a QA has been completed and scored, the QA scorecard is sent to the specialist so they can review and acknowledge their score. ASU needs an automated process where the specialist would receive an email and link for review and acknowledgement or for the specialist to receive the QA scorecard in a format where they could review, and acknowledge in one step. Since we record all voice calls and staff desktop screens, the coaches review the audio and screen recording to score the call; if needed, the coaches are able to pause the recording and go back and listen to a previous section again. The screen capture recordings allow our QA teams the ability to see the specialists entire desktop screen,

and evaluate what the specialist did during the phone call. However, exporting a screen capture video file is not supported. This would be a nice feature to have for QA analysis.

The ASU QA team has the ability to auto-fail a call. However, an auto-fail or a score falling below a certain threshold would result in the QA form not being sent out, and it would not notify the supervisor to speak to the specialist. ASU must have a CCS platform that could send the QA form (failed or below a threshold) to a supervisor directly.

Summary

ASU is an academic institution that is a top 100 in research and teaching and has the largest student base in the United States. The title, The New American University is not just a slogan, but it is the heartbeat that drives ASU to be on the cutting edge of technology. ASU strives to invest in technologies that are not just groundbreaking but technologies that are evolving to meet the dynamic changing culture we live in and have the ability to shift quickly to accommodate new paradigms in higher academic learning.

Included in the Proposer's Response

The proposer **MUST** respond to the following in their proposal:

- **Exhibit A – Scope of Work Questions.** These are determinant questions for the proposer.
 - **Note:** The proposer must contact Lorenzo.Espinoza@asu.edu for the Excel copy of this document.
- **Exhibit B – Minimum Requirements Questionnaire Check sheet.** These are initial qualifying questions for the proposer.
 - **Note:** The proposer must contact Lorenzo.Espinoza@asu.edu for the Excel copy of this document.
- **Transition In/Out Plan**
 - a. A Transition-In/Out Plan which will describe the process for transitioning the University's data to another product in the future, and, in a hosted model, transitioning to another hosting provider. The proposer shall provide a Transition-In/Out Plan that establishes and contains the transition responsibilities, descriptions and schedules for the required tasks. The purpose of the Transition-In/Out Plan is to ensure an efficient and effective transition from the proposer to another service provider or product with minimal disruption to operations. The University expects compliance with the following activities in order to meet this requirement:

No later than 30 calendar days from date of Contract award, contractor must finalize the details of the proposed Transition-In/Out Plan and submit it to the University Project Director for review and approval. The Transition-In/Out Plan must, at a minimum, include:
Goals, expectations and specific objectives of the Transition-In/Out Plan; Description of the methodology and approach for transferring data and other information to another service provider;

Assumptions and dependencies associated with the Transition-In/Out; and

Estimated timelines and milestones for specific tasks throughout the Transition- In/Out Period.

A finalized plan shall be coordinated and drafted between the awarded proposer and ASU for transition in/out services. The proposer must detail a standard or typical transition plan to describe any information on their firm's transition in/out services.

- b. During execution of the approved Transition-In/Out Plan, the Transition-In/Out Team (composed of University staff, contractor, and personnel of another service provider) shall meet regularly to review and update the Transition-In/Out Plan to reflect revisions to schedules, resource requirements, dependencies, and priorities; and to summarize the progress on the Transition-In/Out Plan to date.
- c. The Transition-In/Out Plan submitted by the contractor to the University must be reviewed and approved by University project leadership prior to implementation. Any clarifications or modifications to the Transition-In/Out plan required by the University must be made by Vendor no later than five (5) calendar days from the date of written request.
- d. During a transition-in/out period, contractor will be required to work cooperatively and expeditiously to transfer the existing responsibilities to the University or another service provider.

- **Value-Added Services**

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:

- Training
- Industry partnerships
- Support of ASU's Charter and goals
- Support of Sustainable development, veterans' affairs, initiatives in support of women, wellness, and our changing regional demographics.
- Support and enhance of ASU's reputation as an innovative, foundational model for the New American University
- Commitment to provide significant financial and non-financial support for the University and its signature programs.
- Any other goods or services your company provides

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. Please reply directly underneath each item below in Section VII for ease of evaluation.

1. The proposer shall present evidence that the firm or its officers have been engaged for at least the past five (5) years in providing services as listed in this Request for Proposal.
2. The proposer must provide a minimum of three (3) references, a description of recent project and/or experience in providing similar services as described in this RFP, including institution size. References should be verifiable and able to comment on the firm's experience, with a preference for references receiving services similar to those described in this Proposal. Include the name, title, telephone number, and email address of the individual at the organization most familiar with the Proposer.
3. The proposer must provide details if their firm, or any member of their firm, been declared in default, suspended, terminated or removed from a contract or job related to the services their firm provides in the regular course of business within the last five (5) years. If so, please explain how it was handled.
4. 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 a response to this section.
5. 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.
6. All key personnel proposed by the firm should have relevant experience, and be fully qualified to successfully provide the services described in the Scope of Work. Provide an organizational chart that provides organizational sections, with the section that will have responsibility for performing this project clearly noted.
7. The proposer must provide primary and secondary contacts for this RFP along with resumes.
8. The proposer must provide their white paper that describes specifications of their system/software, security measure, and other technical information that informs concisely about the complexity of their product.
9. The proposer must provide demonstrated experience in consulting and/or implementing large, scalable technology solutions at large institutions, similar to size and scope of ASU. Higher education experience is preferred similar to the size and

scope of ASU.

10. The proposer shall 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 and matches as close as possible to all components outlined within Section V Specifications/Scope of Work. The Gantt chart must estimate a project kickoff from January 1, 2020 to June 30, 2020 for full implementation.

11. Financial Statements:

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

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

Firm's Name
Confidential – Financial Statements

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

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

Firm's Name
Confidential – Financial Statements

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 (45%)
2. Response Proposer Qualifications (35%)
3. Response Pricing Schedule (15%)
4. Sustainability Efforts/Sustainability Questionnaire (5%)

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. Any additional costs, fees, and expenses must be detailed in the proposer's proposal. Any additional expenses, not explicitly stated, will not be honored by ASU unless negotiated and agreed upon prior to the start of additional work. ASU is interested in receiving creative and comprehensive pricing matrices, which leverage the proposer's options with regard to the scope and level of service.

Please see **Exhibit C - Pricing Schedule** attached.

- **Note:** The proposer must contact Lorenzo.Espinoza@asu.edu for the Excel copy of this document.

If ASU agrees to reimburse vendor for any travel expenses, all reimbursable travel expenses must be authorized in writing by ASU in advance of the planned travel and must be consistent with ASU Financial Services Policy FIN 421-01, www.asu.edu/aad/manuals/fin/fin421-01.html. If ASU agrees to reimburse vendor for any expenses, vendor will submit all receipts and any required backup documentation to ASU within 60 days after the applicable expenses were incurred. ASU will not be required to reimburse Licensor for any expenses, invoices, or receipts for expenses received after that time. Proposer must acknowledge and accept this provision.

SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS

Format of Submittal

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

- **One (1)** clearly marked hardcopy “original” in 8.5” x 11” double-sided, non-binding form. No metal or plastic binding – may use binder, folder, or clip for easy removal of proposal; and
- **One (1) “single”** continuous (no folders) electronic copy (**flash drive only**), PC readable, labeled and no passwords. (Exception for the single continuous file requirement applies for any Excel file types – please label appropriately).
- Any confidential and/or proprietary documents must be on a separate flash drive and labeled appropriately.
- Proposer must check all flash drives before submitting. Company marketing materials should not be included unless the Request for Proposal specifically requests them. All photos must be compressed to small size formats.

Content of Submittal

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

1. Appendix 1 – RFP Checklist/Cover Page
2. Section XIII – Mandatory Certifications, Voluntary Product Accessibility Template (VPAT), & Supplier Sustainability Questionnaire
3. Section VII – Proposer Qualifications (Maximum 20 pages not including resumes, CVs, and/or Organizational Charts).
4. Section V – Specifications/Scope of Work. Also, include Exhibits A and B in both PDF and Excel format in soft/digital copy.
5. Section IX – Pricing Schedule. Also, include Exhibit C-Pricing Schedule in both PDF and Excel format in soft/digital copy.
6. Exceptions, justification, and alternate language to Section XII, Terms and Conditions.
7. Confidential/Proprietary Justification Letter with Sealed documents, if applicable. Please review instructions under Section IV, page 9, item 9.

SECTION XII – AGREEMENT - TERMS & CONDITIONS

ARIZONA STATE UNIVERSITY LICENSING AGREEMENT FOR CONTACT CENTER SOLUTION

These Terms and Conditions (T&Cs) apply to the following: written offers, purchase orders, and other documents issued by the Arizona Board of Regents for and on behalf of Arizona State University (ASU) to _____ (Supplier) for furnishing equipment, materials, or supplies (Goods) and/or services (Services) to ASU (the Goods/Services) pursuant to the Contact Center Solution Request for Proposal (RFP). These T&Cs together with any Purchase Order issued by ASU (the PO), any other written agreements signed by both parties, and any other documents incorporated by reference therein or herein collectively constitute the Agreement. Any terms not defined in these T&Cs will have the meanings set forth in the Agreement. The Agreement is effective as of _____ (the Effective Date).

1. **Offer and Acceptance.** The Agreement is subject to cancellation by ASU at any time prior to acceptance by Supplier. Supplier accepts all of the Agreement's terms and conditions, without qualification, upon the sooner of the following: any written acceptance by Supplier; or 2) shipment, delivery, or performance of all or any of the Goods/Services. Any term or condition in any invoice, offer, or other document issued by Supplier that modifies, adds to, or changes the Agreement is rejected, and will not be part of the Agreement unless agreed by ASU in writing.
2. **Order of Precedence.** In the event of an inconsistency or conflict between or among the provisions of the Agreement, the inconsistency or conflict will be resolved by giving precedence in the following order: i) the PO; ii) these T&Cs; and iii) any other agreement or document signed by authorized signatories of both the parties.
3. **Modifications.** Any modification to the PO, including changes to quantity, price, terms of payment, delivery terms, specifications, etc. must be in an updated PO signed by the parties. If a delivery must differ from the PO, do not ship, deliver, or perform the Goods/Services and instead contact the appropriate ASU Buyer.
4. **TERM AND TERMINATION.**
 - a. The Term of the Agreement is three (3) years with the option to renew up to two (2) successive one-year Terms. The total Term will not exceed five (5) years. Following the Term, the Agreement may be extended by mutual written agreement.
 - b. ASU may terminate the Agreement, in whole or in part, with or without cause, upon 30 days written notice to Supplier. Subject to the provision of any Transition Services (as defined below), upon termination, Supplier will refund to ASU all prepaid amounts for Goods/Services not delivered or performed. If the Agreement is terminated pursuant to this section, subject to the provision of any Transition Services, ASU will pay Supplier, as full compensation under the Agreement: (1) the portion of Goods/Services delivered or performed and accepted prior to the effective date of termination based on the unit prices in the Agreement, or, if no unit prices are provided, the pro rata amount of the total order price based on the amount delivered or performed; and (2) a reasonable amount, not otherwise recoverable from other sources by Supplier, and as approved by ASU, with respect to the undelivered, unperformed, or unacceptable portion of the Good/Services. In no event will compensation paid previously under the Agreement together with compensation paid under this section exceed the total PO or Agreement price.
 - c. ASU may terminate the Agreement, in whole or in part, if Supplier defaults on any of its obligations in the Agreement and fails to cure such default within 7 days after receiving notice of default from ASU. In the event of such a default, ASU may procure the Goods/Services from other sources and Supplier will be liable to ASU for any excess costs ASU incurs.
 - d. ASU may terminate the Agreement at any time if Supplier files a petition in bankruptcy, or is adjudicated bankrupt; or if a petition in bankruptcy is filed against Supplier and not discharged within 30 days; or if Supplier becomes insolvent or makes an assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law; or if a receiver is appointed for Supplier or its business.
 - e. **Transition Services.** Upon termination of the Agreement or termination of any Services (regardless of the reason for termination), the parties will work in good faith to transition the terminated Services to ASU or its designees, with minimum interruption to ASU's business. At ASU's option, Supplier will continue to provide Services and will provide

transition support at rates consistent with the terms of the Agreement for a period of no longer than 180 days following the termination date (the Transition Period). Supplier will provide the post-termination Services (the Transition Services) at least at the same levels of quality and timeliness of performance as Services were provided prior to termination, in a professional manner, with high quality, and in accordance with industry standards. The parties may, by written agreement, modify the Transition Services to be provided and the length of the Transition Period.

5. **Survival.** All provisions of the Agreement that anticipate performance after the termination of the Agreement, and all provisions necessary or appropriate to interpret and enforce such provisions, will survive termination of the Agreement.
6. **Prices.** All Prices will be as listed in the PO or, if not listed in the PO, will be as otherwise set forth in the Agreement. Unless otherwise specified in the Agreement: 1) all prices are in US Dollars; 2) prices include any cost for shipping, and handling; and 3) prices will include any travel, labor, interest, import/export fees, and other costs associated with providing the Goods/Services. ASU will reimburse Supplier for expenses that are specifically identified in the PO. To obtain reimbursement for pre-approved expenses, Supplier must submit all receipts and any required backup documentation to ASU within 60 days after the applicable expenses were incurred. If any reimbursable expenses include travel expenses, all reimbursable travel expenses must be authorized in writing by ASU in advance of the planned travel and must be consistent with [ASU Financial Services Policy FIN421-01](#).
7. **Settlement Method and Terms.** Payment will be subject to the provisions of Title 35 of the Arizona Revised Statutes, as amended from time to time (ARS), relating to time and manner of submission of claims. ASU's obligation will be payable only and solely from funds appropriated for the purpose of the Agreement. After delivery and acceptance of the Goods/Services, Supplier will submit an acceptable invoice to ASU. Invoices must be itemized, reference the Agreement or PO number, and include sufficient detail to document the invoiced amount. Unless otherwise specified on the PO, ASU will pay Supplier for the Goods/Services delivered and accepted net 45 days after receipt by ASU of an invoice meeting the requirements of this section.
8. **Taxes.** Unless otherwise specified in the Agreement, prices will include all taxes and fees, including, without limitation, sales, use, or excise taxes, import duties, value added taxes, permit fees, license fees, or similar charges (Taxes). Taxes do not include ASU income taxes or taxes related to ASU's employees.
9. **Inspection.** Supplier will supply the Goods/Services to ASU exactly as specified in the Agreement. The Goods/Services will meet the highest and best industry practices. ASU will have the right to inspect any Goods/Services prior to and a reasonable amount of time after delivery. If ASU determines that any Goods/Services are incomplete, defective, or not in compliance with the specifications or other requirements of the Agreement, ASU may reject such Goods/Services in whole or in part.
10. **Warranties.** In addition to any implied warranties, Supplier warrants to ASU that: 1) the Goods/Services will be free from any defects in design, workmanship, materials, or labor; 2) all of the Services will be performed in a professional and workmanlike manner and in conformity with highest and best industry standards by persons reasonably suited by skill, training and experience for the type of services they are assigned to perform; 3) Supplier will comply, and will be responsible for ensuring Supplier Parties, as defined below, comply with all applicable laws, rules, and regulations in the performance of the Agreement; 4) Supplier owns or has sufficient rights in the Goods/Services that they do not infringe upon or violate any Intellectual Property, as defined below, of any third parties, and are free and clear of any liens or encumbrances; 5) any data, code, or software developed or delivered by Supplier to ASU will not contain any viruses, worms, Trojan Horses, or other disabling devices or code; 6) all sensitive data, personal data, and personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII) provided by Supplier to ASU was obtained legally and Supplier has obtained all requisite permissions from the individuals whose PII is being provided for (a) Supplier to provide the PII to ASU, and (b) ASU to use the PII for the purposes and in the jurisdictions set forth in the Agreement; 7) the prices of Goods/Services in the Agreement are the lowest prices at which these or similar goods or services are sold by the Supplier to similar customers in similar quantities. In the event of any price reduction between execution of the Agreement and delivery of the Goods/Services, ASU shall be entitled to such reduction, and 8) all Goods/Services delivered by Supplier will conform to the specifications, drawings, and descriptions set forth in the Agreement, and to any samples furnished by Supplier. In the event of a conflict among the specifications, drawings, samples, and description, the specifications will govern.

11. **Indemnification.** Supplier will indemnify, defend, save and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents and employees (collectively, Indemnitee) for, from, and against any and all claims, actions, liabilities, damages, losses, or expenses (including court costs, attorneys' fees, and costs of claim processing, investigation, and litigation) for bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by (i) the negligent or willful acts or omissions of Supplier, or any of its owners, officers, directors, members, managers, agents, employees, contractors or subcontractors at all tiers (together with Supplier, the Supplier Parties); (ii) a breach of the Agreement; or (iii) failure to comply with any applicable law, rule, or regulation. Supplier will be responsible for primary loss investigation, defense and judgment costs where this indemnification is applicable.
12. **Responsibility.** Each party is responsible for the negligent or willful acts or omissions of its employees and contractors when acting under such party's direction and supervision. In addition, Supplier is responsible to ASU for compliance with the Agreement by the Supplier Parties. ASU recognizes an obligation to pay attorneys' fees or costs only when assessed by a court of competent jurisdiction. Notwithstanding the terms of the Agreement or any other document: (i) other than for employees and contractors acting under ASU's direction and supervision, ASU is not responsible for any actions of any third parties, including its students; and (ii) no person may bind ASU unless they are an authorized signatory in PUR-202.
13. **Intellectual Property Ownership.** All Intellectual Property (as defined below) that Supplier or any of the Supplier Parties make, conceive, discover, develop or create, either solely or jointly with any other person or persons including ASU, specifically for or at the request of ASU in connection with the Agreement (Contract IP), will be owned by ASU. To the extent any Contract IP is not considered work made for hire for ASU (or if ownership of all rights therein does not otherwise vest exclusively in ASU), Supplier hereby irrevocably assigns, and will cause the Supplier Parties to so assign, without further consideration, to ASU all right, title and interest in and to all Contract IP, including all copyright rights of ownership. Intellectual Property means all ASU Data, as defined below, any and all inventions, designs, original works of authorship, formulas, processes, compositions, programs, databases, data, technologies, discoveries, ideas, writings, improvements, procedures, techniques, know-how, and all patent, trademark, service mark, trade secret, copyright and other intellectual property rights (and goodwill) relating to the foregoing. Supplier will make full and prompt disclosure of the Contract IP to ASU. Supplier will, and will cause the Supplier Parties to, as and when requested by ASU, do such acts, and sign such instruments to vest in ASU the entire right, title and interest to the Contract IP, and to enable ASU to prepare, file, and prosecute applications for, and to obtain patents and/or copyrights on, the Contract IP, and, at ASU's expense, to cooperate with ASU in the protection and/or defense of the Contract IP.
14. **Supplier's Intellectual Property.** Supplier will retain ownership of its pre-existing Intellectual Property, including any that may be incorporated into the Contract IP, provided that Supplier informs ASU in writing before incorporating any pre-existing Intellectual Property into any Contract IP. Supplier hereby grants to ASU a perpetual, irrevocable, royalty-free, worldwide right and license (with the right to sublicense), to freely use, make, have made, reproduce, disseminate, display, perform, and create derivative works based on such pre-existing Intellectual Property as may be incorporated into the Contract IP or otherwise provided to ASU in the course of performing under the Agreement.
15. **Data Use, Ownership, and Privacy.** The terms of this section apply if Supplier receives, has access to, stores, or analyzes any ASU Data (as defined below). As between the parties, ASU will own, or retain all of its rights in, all data and information that ASU provides to Supplier, as well as all data and information managed by Supplier on behalf of ASU, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to the Agreement, even if generated by Supplier, as well as all data obtained or extracted through ASU's or Supplier's use of such data or information (collectively, ASU Data). ASU Data also includes all data and information provided directly to Supplier by ASU students and employees, and includes personal data, metadata, and user content.

ASU Data will be ASU's Intellectual Property and Supplier will treat it as ASU Confidential Information (as defined below). Supplier will not use, access, disclose, or license, or provide to third parties, any ASU Data, except: (i) to fulfill Supplier's obligations to ASU hereunder; or (ii) as authorized in writing by ASU. Without limitation, Supplier will not use any ASU Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, ASU's prior written consent. Supplier will not, directly or indirectly: (x) attempt to re-identify or de-aggregate de-identified or aggregated information; or (y) transfer de-identified and aggregated information to any third party unless that third party agrees not to attempt re-identification or de-aggregation. For ASU Data to be considered de-identified, all direct and indirect personal identifiers must be removed, including names, ID numbers, dates of birth, demographic information, location information, and school information. Upon request by ASU, Supplier will deliver, destroy, and/or make available to ASU, any or all ASU Data.

16. **Nondisclosure and Trade Secrets.** Supplier may receive (or has received) from ASU and otherwise be exposed to confidential and proprietary information relating to ASU's business practices, strategies, and technologies, ASU Data, as well as confidential information of ASU necessary to perform and/or provide the Goods/Services (collectively, ASU Confidential Information). ASU Confidential Information may include, but is not limited to, confidential and proprietary information supplied to Supplier with the legend "ASU Confidential and Proprietary," or other designations of confidentiality. As between Supplier and ASU, the ASU Confidential Information is the sole, exclusive, and valuable property of ASU. Accordingly, Supplier will not reproduce or otherwise use any of the ASU Confidential Information except in the performance or provision of the Goods/Services, and will not disclose any of the ASU Confidential Information in any form to any third party, either during or after the Term, except with ASU's prior written consent. Upon termination of the Agreement, Supplier will cease using, and will return to ASU, all originals and all copies of the ASU Confidential Information, in all forms and media, in Supplier's possession or under Supplier's control.

Supplier will not disclose or otherwise make available to ASU any confidential information of Supplier or received by Supplier from any third party.

Supplier will have no obligation to maintain as confidential ASU Confidential Information (other than ASU Data) that Supplier can show: (i) was already lawfully in the possession of or known by Supplier before receipt from ASU; (ii) is or becomes generally known in the industry through no violation of the Agreement or any other agreement between the parties; (iii) is lawfully received by Supplier from a third party without restriction on disclosure or use; (iv) is required to be disclosed by court order following notice to ASU sufficient to allow ASU to contest such order; or (v) is approved in writing by ASU for release or other use by Supplier.

17. **Information Security.** This section applies 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) Supplier is collecting PII or ASU Data via a link on an ASU.edu or another ASU managed webpage.

All systems, software, services, and devices that store, transmit, or otherwise process ASU Data (each, a System) must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable laws, rules, and regulations. ASU Data means: all data and information that ASU provides to Supplier, as well as all data and information managed by Supplier on behalf of ASU, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to this Agreement, even if generated by Supplier, as well as all data obtained or extracted through ASU's or Supplier's use of such data or information. ASU Data also includes all data and information provided directly to Supplier by ASU students and employees, and includes personal data, metadata, and user content.

a. With respect to each System, Supplier and its contractors at all tiers (directly and through their third party service providers) will meet the following requirements:

1. Access Control. Control access to ASU's resources, including ASU Data, limiting access to legitimate business need based on an individual's job-related assignment, approve and track access to ensure proper usage and accountability, and make such information available to ASU for review, upon ASU's request.
2. Incident Reporting. Report information security incidents that affect ASU Data immediately to ASU (including those that involve information disclosure incidents, unauthorized disclosure of ASU Data, successful network intrusions, malware infection, and unauthorized access or modifications).
3. Off Shore. Ensure (i) that all development or modification of software for ASU is performed only within the borders of the United States, and (ii) all ASU Data (including any backup copies) are stored, accessed from, and otherwise processed only within the borders of the United States.
4. Patch Management. Carry out updates and patch management for all Systems in a timely manner and to the satisfaction of ASU. Updates and patch management must be deployed using an auditable process that can be reviewed by ASU upon ASU's request.
5. Encryption. Ensure all Systems use an industry standard encryption protocol for sensitive data, personal data, or

personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII), in transit and at rest (as documented in NIST 800-57, or equivalent).

6. Notifications. Notify ASU immediately if Supplier receives any kind of subpoena for or involving ASU Data, if any third party requests ASU Data, or if Supplier has a change in the location or transmission of ASU Data. All notifications to ASU required in this Information Security paragraph will be sent to ASU Information Security at Infosec@asu.edu, in addition to any other notice addresses in this Agreement.
 7. Backup and Restoration. Ensure that all ASU Data is available and accessible, and that adequate systems are in place to restore the availability and accessibility of all ASU Data in a timely manner in the event of a physical or technical threat.
 8. Privacy by Design. When developing, designing, selecting, and using Systems for processing sensitive data, personal data, or personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII), Supplier will, with due regard to the state of the art, incorporate and implement data privacy best practices.
- b. In addition to Section 17(a) above, the following provisions apply if: (i) Supplier receives, stores, or analyzes ASU Data (including if the data is not online); or (ii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data:
1. Third Party Security Audits. Complete certified third party audit (such as SOC2 Type II or substantially equivalent) in accordance with then current industry standards, which audits are subject to review by ASU upon ASU's request. Currently, no more than two audits per year are required.
 2. Penetration Tests. Perform periodic third party scans, including penetration tests, for unauthorized applications, services, code, and system vulnerabilities on each System in accordance with industry standards and ASU standards (as documented in [NIST 800-115](#) or equivalent), and Supplier must provide proof of testing to ASU upon ASU's request.
 3. Vulnerability Scanning. All web-based Systems are required to have a remediation plan and third party web application security scans in accordance with then current industry best practices or when required by applicable industry regulations or standards. Supplier must correct weaknesses within a reasonable period of time, consistent with applicable industry regulations or standards, and consistent with the criticality of the risk, and Supplier must provide proof of testing to ASU upon ASU's request.
- c. In addition to Sections 17(a)-(b) above, the following provision applies if: (i) ASU is purchasing or leasing software, or processing a software renewal; (ii) Supplier is creating any code for ASU; or (iii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data:
1. ASU Rights. Allow ASU (directly or through third party service providers) to scan and/or penetration test any System regardless of where it resides.
- d. In addition to Sections 17(a)-(c) above, the following provision applies if: (i) ASU is purchasing or leasing software, or processing a software renewal; (ii) Supplier is creating any code for ASU; (iii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data; or (iv), Supplier is collecting PII or ASU Data via a link on an ASU.edu or other ASU managed webpage:
1. Secure Development. Use secure development and coding standards including secure change management procedures in accordance with industry standards. Prior to releasing new software versions, Supplier will perform quality assurance testing and penetration testing and/or scanning. Supplier will provide to ASU for review, upon ASU request, evidence of a secure software development life cycle (SDLC).
18. **Privacy; No Waivers or End User Agreements**. Supplier will not require any ASU faculty, staff, or students to waive any privacy rights (including under FERPA or the European Union's General Data Protection Regulation (GDPR)) as a condition for receipt of any Goods/Services, and any attempt to do so will be void. If Supplier requires ASU faculty, staff

or students to accept a clickwrap, click-through, end user license, or other similar agreement (End User Agreement), the terms of the End User Agreement that conflict or are inconsistent, with the terms of the Agreement or ASU's Privacy Statement will be void.

19. **Background Checks.** Supplier will exclude from any direct participation in Supplier's performance under the Agreement, any unqualified persons. In addition, at the request of ASU, Supplier will, at Supplier's expense, conduct reference checks and employment, education, SSN trace, National Sex Offender Registry, and criminal history record checks (collectively, Screenings) on requested persons employed or contracted by Supplier to perform work under the Agreement. Supplier will maintain as part of the records Supplier is required to maintain hereunder, all Screening information and all documentation relating to work performance for each employee or contractor who performs work hereunder. Supplier will abide by all applicable laws, rules and regulations including the Fair Credit Reporting Act and any equal opportunity laws, rules, and regulations.
20. **Payment Card Industry Data Security Standard.** The terms of this section apply if Supplier is processing credit or debit card transactions as part of the Agreement. For e-commerce business and/or payment card transactions, Supplier will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI Security Standards), and be solely responsible for security and maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.

Supplier will, at all times during the Term, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Supplier will provide attestation of compliance to ASU annually by delivering to ASU current copies of the following: (i) Supplier's "Attestation of Compliance for Onsite Assessments – Service Providers;" (ii) an attestation that all ASU locations are being processed and secured in the same manner as those in Supplier's "PCI Report on Compliance;" and (iii) a copy of Supplier's PCI Report on Compliance cover letter. Supplier will notify ASU immediately if Supplier becomes non-compliant, and of the occurrence of any security incidents (including information disclosure incidents, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities).

Supplier's services must include the following:

- a. Supplier maintains its own network operating on its own dedicated infrastructure. Supplier's network includes a firewall that (i) includes access control rules that separate Supplier's PCI network from ASU, and (ii) restricts any communication between Supplier's network devices and ASU systems.
 - b. Supplier treats the ASU network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on ASU's network, and ASU has no ability to decrypt cardholder data.
 - c. All devices must be SRED (secure reading and exchange of data), EMV (Europay, MasterCard and VISA) and PTS POI compliant.
21. **Americans with Disabilities Act and Rehabilitation Act.** To the extent applicable, Supplier will comply with all applicable provisions of the Americans with Disabilities Act, the Rehabilitation Act of 1973, and all applicable federal regulations, as amended from time to time (ADA Laws). All electronic and information technology and products and services to be used by ASU faculty/staff, students, program participants, or other ASU constituencies must be compliant with ADA Laws. Compliance means that a disabled person can acquire the same information, engage in the same interactions, and enjoy the same services as a nondisabled person, in an equally effective and integrated manner, with substantially equivalent ease of use.
22. **Foreign Corrupt Practices Act/UK Bribery Act/ Local Anti-corruption Law Compliance.** Supplier warrants that it is familiar with the U.S. laws prohibiting corruption and bribery under the U.S. Foreign Corrupt Practices Act and the United Kingdom laws prohibiting corruption and bribery under the UK Bribery Act. In connection with Supplier's work under the Agreement, Supplier will not offer or provide money or anything of value to any governmental official or employee or any candidate for political office in order to influence their actions or decisions, to obtain or retain business arrangements, or to secure favorable treatment in violation of the Foreign Corrupt Practices Act, the UK Bribery Act, or any other local

anti-corruption law, either directly or indirectly. Any breach of the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, or other local anti-corruption law, will be a material breach of the Agreement.

23. **Export Controls.** If any of the Goods/Services are export-controlled under the U.S. Export Administration Regulations, U.S. International Traffic in Arms Regulations, or through the sanctions and embargoes established through the Office of Foreign Assets Control (collectively, the Export Control Laws), Supplier will provide ASU with written notification that identifies the export-controlled Goods/Services and such Goods/Services export classification. None of the work undertaken pursuant to the Agreement will require either party to take or fail to take any action that would cause a violation of any of the Export Control Laws. The parties will cooperate to facilitate compliance with applicable requirements of the Export Control Laws.
24. **Assignment.** Supplier may not transfer or assign the Agreement or any of Supplier's rights or obligations thereunder, either directly or indirectly, or by operation of law, without ASU's prior written consent, and any attempt to the contrary will be void.
25. **Governing Law and Venue.** The Agreement will be governed by the laws of the State of Arizona without regard to any conflicts of laws principles. ASU's obligations hereunder are subject to the regulations/policies of the Arizona Board of Regents. Any proceeding arising out of or relating to the Agreement will be conducted in Maricopa County, Arizona. Each party consents to such jurisdiction, and waives any objection it may now or hereafter have to venue or to convenience of forum.
26. **Packaging.** Supplier will package the Goods in accordance with good commercial practice. Each shipping container will be clearly and permanently marked as follows: (i) Supplier's name and address; (ii) ASU's name, address, and purchase order number; (iii) container number and total number of containers, e.g., box 1 of 4 boxes; and (iv) the number of the container bearing the packing slip. Supplier will bear cost of packaging unless otherwise provided.
27. **Shipment Under Reservation Prohibited.** Supplier will not ship the Goods under reservation and no tender of a bill of lading will operate as a tender of the Goods.
28. **Title and Risk of Loss.** The title and risk of loss of the Goods will not pass to ASU until they are delivered, received, and the contract of coverage has been completed. All risk of transportation and all related charges will be the responsibility of Supplier. Supplier will insure and file all claims for visible and concealed damage. ASU will notify Supplier promptly of any damaged Goods and will assist Supplier in arranging for inspection. Notice of rejection may be made to Supplier at any time within 1 month after delivery to ASU.
29. **No Replacement of Defective Tender.** Every tender of Goods will fully comply with all provisions of the Agreement as to time of delivery, quantity, quality, and the like. If a tender is made that does not fully conform, this will constitute a breach and Supplier will not have the right to substitute a conforming tender.
30. **Business Continuity Plan.** If requested by ASU, Supplier will provide to ASU, within 30 days after such request, a comprehensive plan for continuing the performance of its obligations during a Public or Institutional Emergency (the Business Continuity Plan). The Business Continuity Plan, at a minimum, will address the following: 1) identification of response personnel by name; 2) key succession and performance responses in the event of sudden and significant decrease in workforce; 3) contingency plans for the Supplier to continue the performance of its obligations under the Agreement, despite the emergency and 4) if Supplier will store, have access to, or otherwise process any ASU Data, a data recovery plan that includes the following: identification of data recovery personnel by name, how ASU Data will be recovered, recovery point and recovery time objectives, and steps to be taken to recover ASU Data. If ASU requires a data recovery plan, upon ASU's request, Supplier will provide ASU with evidence that Supplier annually tests the data recovery plan. In the event of a Public or Institutional Emergency, Supplier will implement the applicable actions set forth in the Business Continuity Plan and will make other commercially practicable efforts to mitigate the impact of the event. For clarification of intent, Supplier will not be entitled to any additional compensation or extension of time by virtue of having to implement a Business Continuity Plan, unless otherwise agreed to by ASU in writing. A Public or Institutional Emergency means a natural or human made event that creates a substantial risk to the public, that causes or threatens death or injury to the general public, or that causes a significant disruption to the day-to-day business operations of ASU.
31. **Gratuities.** Supplier will not give or offer any gratuities, in the form of entertainment, gifts or otherwise, or use an agent or representative of Supplier to give or offer a gratuity, to any officer or employee of the State of Arizona with a view toward securing an agreement or securing favorable treatment with respect to the awarding or amending, or the making of any

determinations with respect to the performing of such Agreement. If ASU determines that Supplier has violated this section, ASU may, by written notice to Supplier, cancel the Agreement. If the Agreement is canceled by ASU pursuant to this section, ASU will be entitled, in addition to any other rights and remedies, to recover or withhold the amount of the costs incurred by Supplier in providing gratuities.

- 32. Modifications.** The Agreement may be modified or rescinded only by a writing signed by both parties.
- 33. Interpretation-Parol Evidence.** The Agreement is intended by the parties as a final expression of their agreement and is intended to be a complete and exclusive statement of the terms of their agreement. No course of prior dealings between the parties and no usage of the trade will be relevant to supplement or explain any term used in the Agreement. Acceptance or acquiescence in a course of performance rendered under the Agreement will not be relevant to determine the meaning of the Agreement even though the accepting or acquiescing party has knowledge of the nature of the performance and opportunity for objection.
- 34. No Waiver.** No waiver by ASU of any breach of the provisions of the Agreement by Supplier will be construed to be a waiver of any future breach or bar ASU's right to insist on strict performance of the Agreement.
- 35. Assignment of Anti-Trust Overcharge Claims.** In actual economic practice, overcharges resulting from anti-trust violations are borne by the ultimate purchaser. Therefore, Supplier hereby assigns to ASU any and all claims for such overcharges.
- 36. Sales and Use Tax.** Supplier will comply, and require all of the Supplier Parties to comply, with all applicable state and sales excise tax laws and compensation use tax laws and all amendments to same. Supplier will indemnify, defend, and hold harmless ASU, for, from, and against any and all claims and demands made against it by virtue of the failure of Supplier or any subcontractor to comply with the provisions of any or all tax laws and amendments. ASU is not exempt from state sales excise tax and compensation use tax.
- 37. Parking.** Supplier will obtain all parking permits and/or decals required while performing any work on ASU premises. If needed, Supplier should contact ASU Parking and Transit, <http://cfo.asu.edu/pts>.
- 38. Campus Deliveries and Mall Access.** Supplier will familiarize itself with ASU parking, campus delivery options, and loading zones. Not all campus buildings are directly accessible and some require Supplier to unload at lots or loading areas that may not be adjacent to the delivery or work location. As a result, Supplier must then transport Goods by using electric style golf carts, dolly, or other manual device across pedestrian malls. Many campuses include features and pedestrian malls that may have limited access for Supplier vehicle and carts. Walk-Only Zones prohibit access to all wheeled traffic during enforcement times, and deliveries or work requiring vehicular or cart access may need to be arranged outside of enforcement times. For details about parking permits, supplier permits, loading zones, mall access, and pedestrian mall restrictions, go to <http://cfo.asu.edu/pts>. For additional information, go to <http://walk.asu.edu>.
- 39. Health Insurance Portability and Accountability Act.** To the extent applicable, Supplier will abide by all laws and regulations that protect the privacy of healthcare information to which Supplier obtains access under the Agreement. Certain portions of the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as codified at 42 U.S.C. § 1320d through d-8, and the federal privacy regulations as contained in 45 CFR Part 164 may apply to Supplier and ASU, and their relationships and operation under the Agreement. If necessary, Supplier and ASU will enter into a standard Business Associate Agreement, and any other required HIPAA agreements. To the extent the terms thereof relate to Supplier's performance under the Agreement, the provisions of the Business Associate Agreement will control.
- 40. Liens.** All Goods/Services delivered and performed under the Agreement will be free of all liens and, if ASU requests, Supplier will deliver to ASU a formal release of all liens.
- 41. Performance and Payment Bonds.** At the request of ASU, Supplier will provide and pay for performance and payment bonds. Bonds will cover the faithful performance (100%) of the Agreement and the payment of all obligations (100%) thereunder, in such form as ASU may prescribe. Supplier will deliver the required bonds to ASU not later than the date of executing the Agreement. Supplier will require the attorney in fact who executes the required bonds on behalf of surety to affix thereto a certified and current copy of his/her power of attorney indicating the monetary limit of such power. Surety will be a company licensed to do business in the State of Arizona and will be acceptable to ASU. Supplier will increase the

bond amount to include any change order, at 100% of the total value amount of each change order.

- 42. Price Adjustment.** ASU normally considers price changes at the end of one contract period and the beginning of another. Price change requests will be supported by evidence of increased costs to Supplier. ASU will not approve price increases that will merely increase gross profitability of Supplier at the expense of ASU. Price change requests will be a factor in the contract extension review process. ASU will determine whether any requested price increase or an alternate option is in the best interest of ASU. Any price adjustment to the Agreement will require an updated PO.
- 43. Academic Freedom and Accreditation.** ASU will maintain ultimate authority over all curriculum. Nothing in the Agreement will limit ASU's academic freedom or require ASU to violate any of the policies, standards, and requirements of ABOR or any accrediting entities.
- 44. Essence of Time.** Time will be of the essence as to matters contemplated by the Agreement.
- 45. Non-Discrimination.** The parties will comply with all applicable laws, rules, regulations, and executive orders governing equal employment opportunity, immigration, and nondiscrimination, including the Americans with Disabilities Act. **If applicable, the parties will abide by the requirements of 41 CFR §§ 60- 1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability.**
- 46. Conflict of Interest.** If within 3 years after the execution of the Agreement, Supplier hires as an employee or agent any ASU representative who was significantly involved in negotiating, securing, drafting, or creating the Agreement, then ASU may cancel the Agreement as provided in ARS § 38-511.
- 47. Arbitration.** The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to ARS § 12-133.
- 48. Dispute Resolution.** If a dispute arises under the Agreement, the parties will exhaust all applicable administrative remedies provided for under Arizona Board of Regents Policy 3-809.
- 49. Records.** To the extent required by ARS § 35-214, Supplier will retain all records relating to the Agreement. Supplier will make those records available at all reasonable times for inspection and audit by ASU or the Auditor General of the State of Arizona during the term of the Agreement and for 5 years after the completion of the Agreement. The records will be provided at ASU in Tempe, Arizona, or another location designated by ASU on reasonable notice to Supplier.
- 50. Failure of Legislature to appropriate.** In accordance with ARS § 35-154, if ASU's performance under the Agreement depends on the appropriation of funds by the Arizona Legislature, and if the Legislature fails to appropriate the funds necessary for performance, then ASU may provide written notice of this to Supplier and cancel the Agreement without further obligation of ASU. Appropriation is a legislative act and is beyond the control of ASU.
- 51. Weapons, Explosives, and Fireworks.** ASU's Weapons, Explosives, and Fireworks Policy prohibits the use, possession, display or storage of any weapon, explosive device or fireworks on all land and buildings owned, leased, or under the control of ASU or its affiliated entities, in all ASU residential facilities (whether managed by ASU or another entity), in all ASU vehicles, and at all ASU or ASU affiliate sponsored events and activities, except as provided in ARS § 12- 781, or unless written permission is given by ASU's Police Chief or a designated representative. Supplier will notify all persons or entities who are employees, officers, subcontractors, consultants, agents, guests, invitees or licensees of Supplier of this policy and Supplier will enforce this policy against all such persons and entities.
- 52. Confidentiality.** ASU, as a public institution, is subject to ARS §§ 39-121 to 39-127 regarding public records. Any provision regarding confidentiality is limited to the extent necessary to comply with Arizona law.
- 53. Indemnification and Liability Limitations.** Because ASU is a public institution, any indemnification, liability limitation, releases, or hold harmless provisions are limited as required by Arizona law, including Article 9, Sections 5 and 7 of the Arizona Constitution and ARS §§ 35-154 and 41-621. ASU's liability under any claim for indemnification is limited to claims

for property damage, personal injury, or death to the extent caused by acts or omissions of ASU.

- 54. Advertising, Publicity, Names and Marks.** Supplier will not do any of the following, without, in each case, ASU's prior written consent: (i) use any names, service marks, trademarks, trade names, logos, or other identifying names, domain names, or identifying marks of ASU (ASU Marks), including online, advertising, or promotional purposes; (ii) issue a press release or public statement regarding the Agreement; or (iii) represent or imply any ASU endorsement or support of any product or service in any public or private communication. Any permitted use of ASU Marks must comply with ASU's requirements, including using the ® indication of a registered mark.
- 55. Privacy; Educational Records.** Student educational records are protected by the U.S. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations (FERPA). Supplier will not require any ASU students or employees to waive any privacy rights (including FERPA or the European Union's General Data Protection Regulation (GDPR)) as a condition for receipt of any educational services, and any attempt to do so will be void. Supplier will comply with FERPA and will not access or make any disclosures of student educational records to third parties without prior notice to and consent from ASU or as otherwise provided by law. If the Agreement requires or permits Supplier to access or release any student records, then, for purposes of the Agreement only, ASU designates Supplier as a "school official" for ASU under FERPA, as that term is used in FERPA. In addition, any access or disclosures of student educational records made by Supplier or any Supplier Parties must comply with ASU's definition of legitimate educational purpose in SSM 107-01: Release of Student Information, at <http://asu.edu/aad/manuals/ssm/ssm107-01.html>. If Supplier violates the terms of this section, Supplier will immediately provide notice of the violation to ASU.
- 56. Data Protection.** Supplier will ensure that all services undertaken pursuant to the Agreement are performed in compliance with applicable privacy and data protection laws, rules, and regulations. In addition, Supplier is responsible to ASU for compliance with the Agreement by all Supplier Parties. If Supplier will serve as a Processor of ASU Data that includes Personal Data of Data Subjects in the European Union, Supplier will cooperate with ASU to comply with the GDPR with respect to such Personal Data and Data Subjects. This includes ensuring that all Data Subjects have signed appropriate Consents, and signing and complying with all documents and agreements reasonably requested by ASU, including any data processing agreements. All capitalized terms in this section not otherwise defined in the Agreement are defined in the GDPR.
- 57. Authorized Presence Requirements.** As required by ARS § 41-4401, ASU is prohibited from awarding a contract to any contractor or subcontractor that fails to comply with ARS § 23-214(A) (verification of employee eligibility through the e-verify program). Supplier warrants that it and its subcontractors comply fully with all applicable immigration laws, rules, and regulations that relate to their employees and their compliance with ARS § 23-214(A). A breach of this warranty will be a material breach of the Agreement that is subject to penalties up to and including termination of the Agreement. ASU retains the legal right to inspect the papers of any contractor or subcontractor employee who works hereunder to ensure that the contractor or subcontractor is complying with the above warranty.
- 58. Small Business.** If subcontracting (Tier 2 and higher) is necessary, Supplier will make commercially reasonable efforts to use Small Business (SB) and Small Diverse Business (SDB) in the performance of the Goods/Services. ASU may request a report at each annual anniversary date and at the completion of the Agreement indicating the extent of SB and SDB participation.
- 59. Tobacco Free.** ASU is tobacco-free. For details visit www.asu.edu/tobaccofree.
- 60. Title IX Obligation.** Title IX protects individuals from discrimination based on sex, including sexual harassment. ASU fosters a learning and working environment built on respect and free of sexual harassment. ASU's Title IX Guidance is available online. Supplier will: (i) comply with ASU's Title IX Guidance; (ii) provide ASU's Title IX Guidance to any Supplier Parties reasonably expected to interact with ASU students or employees, in person or online; and (iii) ensure that all Supplier Parties comply with ASU's Title IX Guidance.
- 61. No Boycott of Israel.** To the extent required by ARS § 35-393.01, Supplier certifies it is not currently engaged in a boycott of Israel and will not engage in a boycott of Israel during the Term.
- 62. Insurance Requirements.** Without limiting any liability of 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 in Exhibit A. In addition, Supplier and ASU will reasonably cooperate to reach mutual agreement if the State of Arizona requires modification or variation from the Insurance Requirements.

63. Provision of Goods/Services to ASU Component Units. In addition to providing the Goods/Services to ASU, Supplier will provide some or all of the Goods/Services to each of ASU's Component Units that so requests. Supplier will enter into a Consent and Agreement to be Bound (attached as Exhibit B) with each such requesting Component Unit, and except as may be set forth in the Consent and Agreement to be Bound, Supplier will provide the Goods/Services to each such Component Unit to the same extent and on the same terms provided to ASU under this Agreement. ASU's Component Units are described in ASU's Comprehensive Annual Financial Reports (Note B to Financial Statements).

64. Third Party Arrangements. From time to time, ASU may enter into arrangements with third parties that may require Supplier to work cooperatively with and/or connect and use infrastructure with third parties. On a case-by-case basis, ASU and Supplier will work cooperatively, timely, and in good faith to take such actions as may be necessary or appropriate to give effect to ASU's third party agreements. Supplier will not be bound to terms and conditions of a third party that are different from this Agreement unless expressly agreed in writing. If the third party terms and conditions conflict with this Agreement's terms, impact Supplier's ability to meet service level agreements of this Agreement, or may cause Supplier to incur additional costs, then the parties will enter into good faith negotiations for an amendment to this Agreement prior to Supplier agreeing to compliance with the third party terms and conditions.

65. Independent Contractor. Supplier is an independent contractor. Neither ASU nor Supplier may bind the other. None of the Supplier Parties will be employees, agents, partners, or joint venturers of ASU. None of the Supplier Parties will be eligible for any benefits from ASU, including worker's compensation coverage. Supplier is responsible to ASU for compliance with the Agreement by the Supplier Parties. Supplier will determine Supplier's hours of work, and will provide all tools, equipment, and supplies Supplier determines to be necessary to deliver and perform the Goods/Services. Supplier will maintain all business registrations and licenses required to deliver and perform the Goods/Services. Supplier is using its own knowledge, skill, and technical know-how in the delivery and performance of the Goods/Services and is not being supervised by ASU. The conduct and control of Services lies solely with Supplier, and ASU is interested only in final results.

66. Federal Funding Provisions. If the Agreement involves the use of United States federal funds, including from a government grant or funds from a subcontract at any tier relating to a federal government grant, the following terms apply to the Agreement:

- a. **Byrd Anti-Lobbying Amendment.** If the Agreement is for \$100,000 or more, Supplier will file the certifications required by 31 U.S.C 1352 and associated regulations. Each tier certifies to the tier above that it will not or has not used federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any federal contract, grant, or any other award covered by 31U.S.C. 1352. Each tier will also disclose any lobbying with non-federal funds that takes place in connection with obtaining a federal award. Such disclosures are forwarded from tier to tier up to ASU.
- b. **Debarment & Suspension.** Supplier represents and warrants that neither it nor any of its subcontractors supplying the Goods/Services have either directly or indirectly or through subcontractors, been suspended, debarred, or otherwise excluded from participation in or penalized by any federal or state procurement, non- procurement, or reimbursement program. Supplier affirms that it has confirmed the above statement by checking The System for Award Management (SAM) www.uscontractorregistration.com within 180 days prior to commencing work under the Agreement. Supplier will provide immediate written notice to ASU upon learning that it or any of its subcontractors are under any investigation or proposed action that could result in such exclusion, suspension, or debarment.
- c. **Rights to Inventions Made Under an Agreement or Agreement.** If this Agreement is a "funding agreement" under 37 CFR 401.3, the Parties agree to incorporate by this reference the standard patent rights clause found in 37 CFR 401.14 and any implementing regulations issued by the awarding agency.
- d. **Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.** To the extent any of the provisions of 2 CFR Appendix II to Part 200 apply to this Agreement, such provisions are incorporated by reference.

67. Government Subcontract Provisions. If this order is a subcontract under a U.S. government prime contract, the clauses referenced below of the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulations (DFAR), or the Armed Services Procurement Regulations (ASPR) are incorporated into the Agreement by this reference. Each regulation contains criteria for determining applicability of the regulation to a particular contract.

In the following clauses, the terms "Government" and "Contracting Officer" will mean ASU; the term "Agreement" will mean the Agreement and the term "Contractor" will mean Supplier. Supplier will comply with all applicable federal laws and regulations, including but not limited to Uniform Guidance (2 CFR Part 200) and Debarment and Suspension (45 CFR 620).

For purchases funded with federal funds, the following provisions are incorporated into the Agreement by reference where applicable and form a part of the terms and conditions of the Agreement. Supplier agrees to flow down all applicable clauses to lower-tier entities.

FEDERAL ACQUISITION REGULATIONS (FAR)**

52.202-1 Definitions
52.203-3 Gratuities
52.203-5 Covenant Against Contingent Fees
52.203-6 Restrictions on Subcontractor Sales to the Government
52.203-7 Anti-Kickback Procedures
52.203-12 Limitation on Payments to Influence Certain Federal Transactions
52.204-2 Security Requirements
52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended or Proposed for Debarment
52.211-15 Defense Priority and Allocation Requirements
52.214-27 Price Reduction For Defective Cost or Pricing Data
52.215-1 Instructions to Offerors—Competitive Acquisition.
52.215-2 Audit and Records - Negotiation
52.215-12 Subcontractor Cost or Pricing Data
52.215-13 Subcontractor Cost or Pricing Data – Modifications
52-215-14 Integrity of Unit Prices
52-219-8 Utilization of Small Business Concerns
52-219-9 Small Business Subcontracting Plan
52.222-1 Notice to the Government of Labor Disputes
52.222-4 Contract Work Hours and Safety Standards Act Overtime Compensation
52.222-6 Davis-Bacon Act [Construction Wage Rate Requirements]
52.222-20 Walsh Healey Public Contracts Act [Contracts for Materials, Supplies, Articles, and Equipment Exceeding \$15,000.]
52.222-21 Prohibition of Segregated Facilities
52.222-26 Equal Opportunity
52.222-35 Equal Opportunity for Veterans
52.222-36 Equal Opportunity for Workers with Disabilities
52.222-37 Employment Reports on Veterans
52.222-40 Notification of Employee Rights Concerning Payment of Union Dues or Fees
52.222-41 Service Contract Act of 1965, as Amended
52.222-50 Combating Trafficking in Persons
52.223-3 Hazardous Material Identification and Material Safety Data
52.223-6 Drug-Free Workplace
52.225-1 Buy American Act – Supplies
52.225-13 Restrictions on Certain Foreign Purchases
52.227-1 Authorization and Consent (Alt I in all R&D)
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement
52.227-3 Patent Indemnity
52.227-10 Filing of Patent Applications--Classified Subject Matter
52.227-11 Patent Rights – Ownership by the Contractor (Alt I-V)

- 52.227-13 Patent Rights - Ownership by the Government
- 52.227-14 Rights in Data – General
- 52.233-1 Disputes
- 52.242-1 Notice of Intent to Disallow Costs
- 52.242-15 Stop-work order
- 52.243-1 Changes - Fixed Price (43.205 (a) (1) Alts may apply)
- 52.243-2 Changes - Cost Reimbursement (43.205 (b) (1) Alts may apply)
- 52.244-2 Subcontracts
- 52.244-5 Competition in Subcontracting
- 52.244-6 Subcontracts for Commercial Items
- 52.245-2 Government Property – Installation Operation Services
- 52.246-15 Certificate of Conformance
- 52.247-63 Preference for U.S. Flag Air Carriers
- 52.247-64 Preference for U.S. Flag Commercial Vessels
- 52.249.1 Termination for Convenience of the Government (Fixed Price) less than simplified acquisition threshold
- 52.249-2 Termination for Convenience of the Government (Fixed Price) more than simplified acquisition threshold
- 52.249.4 Termination for Convenience of the Government (Services)
- 52.249-5 Termination for the Convenience of the Government (Educational and Other Nonprofit Institutions)
- 52.249-14 Excusable Delays

DEFENSE FEDERAL ACQUISITION REGULATIONS (DFAR) DFAR CIT. TITLE**

- 252.203-7001 Prohibition on Persons convicted of Fraud or Other Defense-Contract-Related Felonies
- 252.222- 7000 Restrictions on Employment of Personnel
- 252.225-7000 Buy American Act and Balance of Payments program
- 252.227-7013 Rights in Technical Data and Computer Software
- 252.227-7016 Rights in Bid or Proposal Information
- 252.227-7018 Rights in Noncommercial Technical Data and Computer Software
- 252.227-7019 Validation of Asserted Restrictions – Computer Software
- 252.227-7037 Validation Technical Data
- 252.243-7001 Pricing of Agreement Modifications
- 252.244-7000 Subcontracts for Commercial Items and Commercial Components

*Full text of the FAR clauses can be found at <http://www.arnet.gov/far>

**Full text of the DFAR clauses can be found at <http://farsite.hill.af.mil/VDFARs.htm>

68. Notices. All notices and communications required or permitted under this Agreement will be in writing and will be given by personal delivery against receipt (including private courier such as FedEx), or certified U.S. Mail, return receipt requested. All notices and communications will be sent to the addresses below or such other addresses as the parties may specify in the same manner.

To ASU:

Project Manager, Information Technology
 University Technology Office Help Center
 Arizona State University

Mailing Address:

PO Box 876504
 Tempe, AZ 85287-6504

Delivery Address:

1150 E. University Dr.
 Tempe, AZ 85281

With a copy to:

Chief Procurement Officer
 Purchasing and Business Services
 Arizona State University

Mailing Address:

PO Box 875212

To Supplier:

With a copy to:

Tempe, AZ 85287-5212
Delivery Address
1551 S. Rural Rd.
Tempe, AZ 85281

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

- 69. Billing Disputes.** If ASU disputes a charge in good faith on any invoice, ASU may withhold payment of that charge if ASU makes timely payment of all undisputed charges when due and provides Supplier with a written explanation of the reasons for ASU's disputes of the charge within 90 days after receipt by ASU of the invoice for such amount. If Supplier determines, in its good faith, that the disputed charge is valid, Supplier will notify ASU and within 5 business days after Supplier's notification, ASU must pay the charge, unless ASU continues to dispute the charge in good faith.
- 70. ASU's Policies.** All Services will be provided in accordance with ASU's policies, as they may change or be updated. Changes to such policies or standards may directly or indirectly increase or decrease the scope of Services to be provided by Supplier under this Agreement. Where reasonably possible, ASU will collaborate with Supplier on policies and standards that may have a material impact on Supplier, and reasonably listen to Supplier's feedback in an effort to achieve the goals of ASU without introducing new or additional costs to provide the Services. If ASU presents a new or modified policy or standard that a party reasonably believes will materially increase or decrease Supplier's costs to provide the Services, the parties will meet in good faith to amend the Agreement as appropriate. If Supplier believes the impact to be an increase in scope or cost, Supplier will comply with the new or modified policy or standard to the extent possible under this Agreement until the parties can reach an amendment or agreement on how to address full compliance.
- 71. State Purchasing Cooperative.** The Agreement and ASU's Contact Center Solution RFP may be used by state, city, and county governments within the state of Arizona, Arizona state-funded K-20 educational districts and institutions (including charter schools), and the other two state universities governed by the Arizona Board of Regents: University of Arizona, and Northern Arizona University (collectively, the Arizona Entities). Each of the Arizona Entities may purchase some or all of the Goods/Services under the Agreement. ASU will have no liability or responsibility to Supplier or otherwise for purchases of the Goods/Services by the Arizona Entities. Supplier may negotiate different rates, terms, and conditions with the Arizona Entities.
- 72. Administrative Fee.** Supplier will pay ASU an Administrative Fee in the amount of 1% of the gross funds received by Supplier from the Arizona Entities or any other similar entity in any other state. This fee will apply only to contracts entered into after the effective date of the Agreement. The Administrative Fee will apply to any and all Goods/Services provided by Supplier that reference the Agreement or the RFP as the supporting documentation to meet competitive bidding requirements. The Administrative Fee will be calculated based on all sales transacted, minus all taxes and any returns or credits. Supplier will submit the Administrative Fee, along with a quarterly usage report documenting all contract sales, to the ASU Chief Procurement Office within 30 days following the end of each calendar quarter. Each quarterly report at a minimum, will disclose all purchased Goods/Services, prices paid, and quantity, by individual purchasing agency, for all sales within the calendar quarter just ended. The Administrative Fee is payable by Supplier, from Supplier's funds, to ASU.

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

Supplier:

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date Signed: _____

Date Signed: _____

Exhibit A – Insurance Requirements

Exhibit B – Consent and Agreement to Be Bound
Exhibit C – Order Form
Exhibit D – Statement of Work
Exhibit E – Service Level Agreement

EXHIBIT A – 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.

- | | |
|---|-------------|
| • Each Occurrence | \$5,000,000 |
| • Products – Completed Operations Aggregate | \$1,000,000 |
| • Personal and Advertising Injury | \$1,000,000 |
| • Contractual Liability | \$1,000,000 |
| • Fire Legal Liability (only if Agreement is for leasing space) | \$50,000 |

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 \$10,000,000

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 \$5,000,000

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

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

B. **Cancellation; Material Changes.** Cancellation notices will be delivered to ASU in accordance with all policy provisions. Notices required in this Section must be sent directly to ASU Purchasing and Business Services, email Insurance.certificates@asu.edu or mail to PO Box 875212, Tempe, AZ, 85287-5212.

C. **Acceptability of Insurers.** Insurance is to be placed with duly licensed or approved non-admitted insurers in the State of Arizona with an "A.M. Best" rating of not less than A- VII. ASU in no way warrants that the above required minimum insurer rating is sufficient to protect 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.

Exhibit B – Consent and Agreement to be Bound

This Consent and Agreement to be Bound to _____ Agreement (this Consent) is entered into between _____ (Supplier) and _____, an Arizona nonprofit corporation (Company). This Consent is effective as of the date of the last signature below (the Effective Date).

RECITAL

- A. Effective as of _____, the Arizona Board of Regents for and on behalf of Arizona State University (ASU) and Supplier entered into the Arizona State University Licensing Agreement for Contact Center Solution (the Agreement) whereby Supplier contracted to provide ASU with certain Goods/Services, and agreed to provide the same Goods/Services to ASU’s Component Units if the Component Units agreed to be bound by the terms of the Agreement as if they were the customer thereunder. A copy of the Agreement is attached as Schedule A.
- B. Company is a Component Unit of ASU.
- C. Company desires to have access to the Goods/Services under the same terms as ASU, and to agree to be bound by the terms of the Agreement, and Supplier desires to provide the Goods/Services to Company to the same extent as if Company were ASU under the Agreement.
- D. All capitalized terms not defined in this Consent have the definitions set forth in the Agreement.

AGREEMENT

Supplier and Company agree as follows:

- 1. Consent to be Bound. Except as may be set forth in this Consent, Company will be bound by and observe all of the terms, conditions, and covenants of, and to perform all of the duties and obligations of, ASU under and pursuant to the Agreement, as if Company were the customer under the Agreement, and Company hereby executes and delivers the Agreement as a customer thereunder.
- 2. Provision of Services. Except as may be set forth in this Consent, Supplier will provide the Goods/Services to Company to the same extent and on the same terms as if Company were the customer under the Agreement. Each party to this Consent will be liable and responsible to the other for its actions to the same extent that ASU and Supplier are liable and responsible to each other under the Agreement.
- 3. Company Representations. Company represents to Supplier that: (a) it has the right, power, capacity, and authority to execute and deliver this Consent and the Agreement, and to fully and timely perform all of the duties and obligations required by the customer under and pursuant to the Agreement; and (b) the Agreement is a legal, valid, and binding obligation of Company, enforceable by Supplier against Company in accordance with its terms.
- 4. Supplier Registrations. Supplier represents to Company that: (a) it has the right, power, capacity, and authority to execute and deliver this Consent and the Agreement, and to fully and timely perform all of its duties and obligations under and pursuant to this Consent and the Agreement; and (b) the Agreement is a legal, valid, and binding obligation of Supplier, enforceable by Company against Supplier in accordance with its terms.
- 5. Company Specific Provisions. The following apply to Company with respect to the Agreement:
 - a. Company’s authorized contacts for purposes of the Agreement are: _____
 - b. Company is not a public institution. Accordingly, the provisions in the Agreement stating that the customer is a public institution do not apply to Company.
 - c. Company’s address information for notices pursuant to Section 68 of the Agreement is:

6. Other Documents. In addition to entering into this Consent, to the extent reasonably necessary, Company and Supplier will sign such other documents as may be required to obtain the benefits under the Agreement and to receive and deliver the Goods/Services ordered by Company. ASU will have no liability or responsibility for Company's performance under any other document signed by Company.
7. Further Assurances. Each of the parties to this Consent will sign and deliver all such documents, and take all such actions as may be reasonably necessary to effectuate the purposes of this Consent consistent with the intentions of the parties.

Supplier:

_____ **An Arizona nonprofit corporation**

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date Signed: _____

Date Signed: _____

Exhibit C – Order Form

This Order Form is subject to and made in accordance with the Arizona State University Licensing Agreement for Contact Center Solution dated _____ between ASU and Supplier (the Agreement). All capitalized terms not defined herein have the meaning in the Agreement. To the extent any provisions of this Order Form conflict with the provisions of the Agreement, the provisions of the Agreement will control. Any other terms in an Order Form provided by Supplier or on Supplier’s website are expressly rejected.

ASU	Supplier
Arizona Board of Regents for and on behalf of Arizona State University	
Representative:	Representative:
Shipping Address:	Billing Address:

Effective Date	Term	Delivery Method	Payment Terms
			Net-30 upon receipt of invoice

Licensed Materials Description	Quantity	Price
Total License Fees:		

Services Description	Quantity	Price
Total Maintenance Fees:		

Additional Terms

1. If, in this Exhibit C, ASU agrees to reimburse Supplier for any travel expenses, all reimbursable travel expenses must be authorized in writing by ASU in advance of the planned travel and must be consistent with ASU's Financial Services Policy FIN [421-01](#).
2. If, in this Exhibit C, ASU agrees to reimburse Supplier for any expenses, Supplier will submit all receipts and all required backup documentation to ASU within 60 days after the applicable expenses were incurred. ASU will not be required to reimburse Supplier for any expenses, invoices, or receipts for expenses received after that time.

Attachments (include number of pages of each):

1. Exhibit D – Statement of Work
2. Exhibit E – Service Level Agreement

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

Supplier:

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date Signed: _____

Date Signed: _____

Exhibit D – Statement of Work

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

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

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

Supplier:

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

Exhibit E – Service Level Agreement

This Service Level Agreement (SLA) is made in accordance with the Arizona State University Licensing Agreement for Contact Center Solution between _____ (Supplier) and the Arizona Board of Regents for and on behalf of Arizona State University (ASU) effective _____ (the Agreement). To the extent any provision in this SLA conflicts with any provision of the Agreement, the provision of the Agreement will control.

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

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

Supplier:

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

SECTION XIII – MANDATORY CERTIFICATIONS

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

CONFLICT OF INTEREST CERTIFICATION

(Date)

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

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

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

(Firm)

(Address)

(Email Address)

(Signature required)

(Phone)

(Print name)

(Fax)

(Print title)

(Federal Taxpayer ID Number)

FEDERAL DEBARRED LIST CERTIFICATION

Certification Other Responsibility Matters (April 2010)

(Date)

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

(a)

(1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals—

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

(B) (check one) **Have** () or **have not** (), within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

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

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

(ii) The Offeror (check one) **has** () or **has not** (), within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principal," for the purposes of this certification, means an officer; director; owner; partner; or, person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

(b) The Offeror shall provide immediate written notice to the University if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the University may render the Offeror nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the University may terminate the contract resulting from this solicitation for default.

(Firm)

(Address)

(Email Address)

(Signature required)

(Phone)

(Print name)

(Fax)

(Print title)

(Federal Taxpayer ID Number)

ANTI-LOBBYING CERTIFICATION

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

(Date)

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

(a) The definitions and prohibitions contained in the clause, at FAR 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in paragraph (b) of this certification.

(b) The offeror, by signing its offer, hereby certifies to the best of his or her knowledge and belief that on or after December 23, 1989—

(1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of this contract;

(2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the offeror shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the University; and

(3) Offeror will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of \$100,000 shall certify and disclose accordingly.

(c) Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by Section 1352, Title 31, United States Code. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision, shall be subject to a civil penalty of not less than \$10,000, and not more than \$100,000, for each such failure.

(Firm)

(Address)

(Email Address)

(Signature required)

(Phone)

(Print name)

(Fax)

(Print title)

(Federal Taxpayer ID Number)

Voluntary Product Accessibility Template (VPAT)

A Voluntary Product Accessibility Template (VPAT™) is a document that explains how information and communication technology (ICT) products such as software, hardware, electronic content, and support documentation meet (conform to) the [Revised 508 Standards](#) for IT accessibility. VPATs™ help Federal agency contracting officials and government buyers to assess ICT for accessibility when doing market research and evaluating proposals.

Government solicitations which include ICT will specify accessibility requirements, indicating which provisions are required to ensure the deliverable is accessible. A VPAT™ is a good way to address the accessibility requirements defined in the solicitation.

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

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

The proposer must access the current VPAT template by visiting <https://www.section508.gov/sell/vpat> and provide the completed form as part of their proposal, per the instructions of the RFP.

- [Download the current VPAT™ template](#) from the Information Technology Industry Council (ITI) website
- Make it easy to find your product's VPAT™ on your company's website (e.g., link to it on the product description page).

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>

Practice Green health provides basic information and tools for emissions as well:

- <https://practicegreenhealth.org/topics/energy-water-and-climate/climate/tracking-and-measuring-greenhouse-gas-emissions>

Solid Waste

The EPA's pre-built excel file to help measure and track your waste and recycling:

- <http://www.epa.gov/smm/wastewise/measure-progress.htm>

Greenbiz's comprehensive guide to reducing corporate waste:

- <http://www.greenbiz.com/research/report/2004/03/09/business-guide-waste-reduction-and-recycling>

Water Waste

BSR's guide on how to establish your water usage:

- http://www.bsr.org/reports/BSR_Water-Trends.pdf

EPA information about conserving water:

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

Packaging

Links to get you started on sustainable packaging:

- <http://www.epa.gov/oswer/international/factsheets/200610-packaging-directives.htm>
- <http://sustainablepackaging.org/uploads/Documents/Definition%20of%20Sustainable%20Packaging.pdf>

Sustainability Practices

Ideas for alternative transportation programs:

- <http://www.ctaa.org/webmodules/webarticles/articlefiles/SuccessStoriesEmpTranspPrograms.pdf>

The EPA environmentally preferable purchasing guidelines for suppliers:

- <http://www.epa.gov/epp/>

EPA life cycle assessment information:

- <http://www.epa.gov/nrmrl/std/lca/lca.html>

Green Seal green products & services:

- <http://www.greenseal.org/FindGreenSealProductsandServices.aspx?vid=ViewProductDetail&cid=16>

Ecologo cleaning and janitorial products:

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

EPA information on sustainable landscape management:

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

SECTION XIV - SECURITY REVIEW

Security Review Form

Form version: 2018-10-19

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?

<input type="checkbox"/>	High	We don't know who is responsible for the security design of the entire system.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.

<input type="checkbox"/>	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.
<input type="checkbox"/>	Low	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> ● SOC2 Report ● System Development Life Cycle (SDLC)
<input type="checkbox"/>	Addressed	<p>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:</p> <p>_____</p> <p>_____</p>

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.)

<input type="checkbox"/>	High	Sensitive data will be traveling across one or more external connections outside of the ASU data Center without any protection.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Addressed	All sensitive data is encrypted as it travels over each network connection.
<input type="checkbox"/>	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.)
<input type="checkbox"/>	Addressed	This project has no sensitive data.
<input type="checkbox"/>	Addressed	This question is not applicable for this project because all of the following are true: <ul style="list-style-type: none"> ● 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.)

<input type="checkbox"/>	High	Sensitive data will be stored without any protection, on devices available to the general public without logging in.
<input type="checkbox"/>	High	Sensitive data will be stored without encryption at rest, even though PCI or other applicable regulations require it.
<input type="checkbox"/>	Medium	Sensitive data will be stored without encryption, but the devices require a login, and there is no applicable regulation requiring encryption at rest.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Low	Sensitive data is encrypted on disk, but not on backups. There is no applicable regulation requiring encryption at rest.
<input type="checkbox"/>	Addressed	All sensitive data is encrypted at every location where it is stored, including user devices and backups.
<input type="checkbox"/>	Addressed	This project has no sensitive data.
<input type="checkbox"/>	Addressed	This question is not applicable for this project because all of the following are true: <ul style="list-style-type: none"> • 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?

<input type="checkbox"/>	Unknown	<p>***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.***</p> <p>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.</p>
<input type="checkbox"/>	Unknown	<p>***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.***</p> <p>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.</p>
<input type="checkbox"/>	Addressed	<p>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.</p>
<input type="checkbox"/>	Addressed	<p>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.</p>

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

<input type="checkbox"/>	Unknown	Some new or changed servers have not yet been scanned or penetration tested.
<input type="checkbox"/>	High	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
<input type="checkbox"/>	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).
<input type="checkbox"/>	Medium	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
<input type="checkbox"/>	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).
<input type="checkbox"/>	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?

<input type="checkbox"/>	Unknown	At present we don't know if there will be development or QA instances of the web site(s).
<input type="checkbox"/>	Medium	Only a production instance exists. There is no place to test code or changes without impacting live systems and data.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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>).

<input type="checkbox"/>	Unknown	Some web sites have not yet been scanned or penetration tested.
<input type="checkbox"/>	High	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
<input type="checkbox"/>	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).
<input type="checkbox"/>	Medium	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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>.

<input type="checkbox"/> 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.)
<input type="checkbox"/> Medium	The web site has access to sensitive data, but is not rated High.
<input type="checkbox"/> 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.)
<input type="checkbox"/> 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?

<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.)
<input type="checkbox"/>	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.
<input type="checkbox"/>	Addressed	None of the systems in this project have access to a database containing sensitive data.
<input type="checkbox"/>	Addressed	This question is not applicable for this project because all of the following are true: <ul style="list-style-type: none">• 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?

<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Addressed	All systems that require users to identify themselves use standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
<input type="checkbox"/>	Addressed	Access is in compliance with the ASU Privileged account standard: https://docs.google.com/file/d/0B7bqVGx3GJQbaC10bEI0ZndjVVE/
<input type="checkbox"/>	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?

<input type="checkbox"/>	High	One or more servers initiate or accept connections with their peers, but do not verify or otherwise restrict which servers can connect.
<input type="checkbox"/>	High	When a server logs in to another server, a password or other secret is transmitted across a network connection without encryption.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Addressed	The project does not have more than one server, so there is no need for servers to authenticate each other.
<input type="checkbox"/>	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.

<input type="checkbox"/>	Unknown	Status of vendor contract(s) or inclusion of ISO language is presently unknown.
<input type="checkbox"/>	High	There are one or more vendors with whom we do not yet have a contract.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Addressed	There is a contract with each vendor, and each contract includes current ISO language.
<input type="checkbox"/>	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?

<input type="checkbox"/>	High	There are no backups of some or all systems that are relied upon to store data.
<input type="checkbox"/>	Medium	Backups are being made, but the ability to fully restore after a total data loss has not been tested.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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?

<input type="checkbox"/>	Unknown	We do not currently know the status of Disaster Recovery and Business Continuity plans.
<input type="checkbox"/>	High	This is a Mission Critical project but it doesn't currently have Disaster Recovery and Business Continuity plans.
<input type="checkbox"/>	Medium	Disaster Recovery and Business Continuity plans don't exist at this time, however, the project is not Mission Critical.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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

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

<input type="checkbox"/>	HIGH	No logging is performed on any system
<input type="checkbox"/>	High	Some systems do not recognize and log typical attacks, or other unexpected or undesired events.
<input type="checkbox"/>	Medium	Potential security events are logged, but there is no human or automated review of those logs to alert on possible problems.
<input type="checkbox"/>	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 .
<input type="checkbox"/>	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.
<input type="checkbox"/>	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?

<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.

<input type="checkbox"/>	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.
<input type="checkbox"/>	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?

<input type="checkbox"/>	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.
<input type="checkbox"/>	High	One or more software components used within this project have no SDLC.
<input type="checkbox"/>	Medium	An SDLC exists, but it is not written, it is not routinely followed, or it does not include security controls.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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?

<input type="checkbox"/>	High	No vulnerability scanning or penetration testing has been conducted
<input type="checkbox"/>	High	One or more components of new software (other than web sites) have not been vulnerability scanned or penetration tested.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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).
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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?

<input type="checkbox"/>	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.)
<input type="checkbox"/>	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.)
<input type="checkbox"/>	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.

<input type="checkbox"/>	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.
<input type="checkbox"/>	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.)
<input type="checkbox"/>	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.)
<input type="checkbox"/>	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.)
<input type="checkbox"/>	Low	Users are required to enable or install other plug-ins or media players not listed above. (Please describe in notes below.)
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.)

<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

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 the server is listening

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

Additional Info

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

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

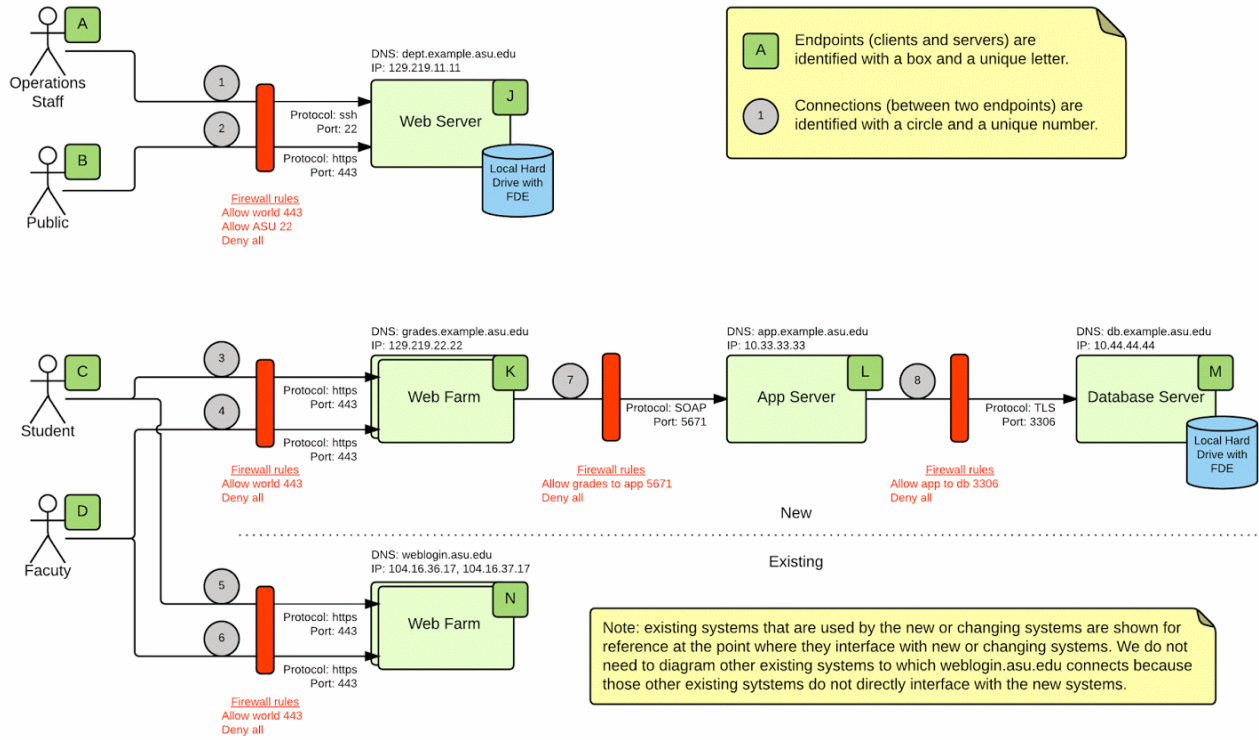
It is not necessary to show disk drives that are physically within a single server. However network shares are most likely part of a file server, and the file server should also be shown as a distinct endpoint.

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

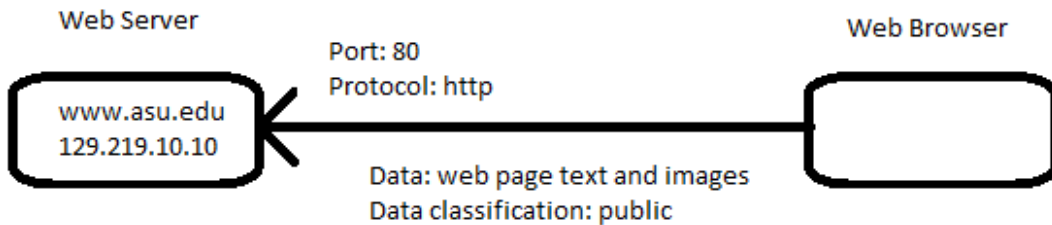
EXAMPLES:

Example Security Architecture Diagram

Revised 2015-07-31



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.



APPENDIX 1 - RFP CHECKLIST/COVER PAGE

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):

<input type="checkbox"/>	Section 1	RFP Checklist/Cover Page, Mandatory Certifications, Voluntary Product Accessibility Template (VPAT), & Supplier Sustainability Questionnaire.
<input type="checkbox"/>	Section 2	Proposer Qualifications, Section VII (Maximum 20 pages not including resumes, CVs, and/or Organizational charts).
<input type="checkbox"/>	Section 3	Response to the Specifications/Scope of Work, Section V. Also Include: <ul style="list-style-type: none"> • Attachments 1-7 (Provide both PDF and Excel files in soft/digital copy)
<input type="checkbox"/>	Section 4	Price Schedule, Section IX. Also include: <ul style="list-style-type: none"> • Attachment A Pricing Schedule
<input type="checkbox"/>	Section 5	Exceptions to Terms and Conditions, Section XII
<input type="checkbox"/>	Section 6	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)

<input type="checkbox"/>	RFP 341904 (PDF Document)
<input type="checkbox"/>	All RFP Addendums (PDF Document)
<input type="checkbox"/>	Attachment 1 (Excel Document)
<input type="checkbox"/>	Attachment 2 (Excel Document)
<input type="checkbox"/>	Attachment 3 (Excel Spreadsheet)
<input type="checkbox"/>	Attachment 4 (Excel Spreadsheet)
<input type="checkbox"/>	Attachment 5 (Excel Document)

<input type="checkbox"/>	Attachment 6 (Excel Document)
<input type="checkbox"/>	Attachment 7 (Excel Document, within the RFP 341901 Document)
<input type="checkbox"/>	Attachment A – Pricing Schedule (Excel 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 #