November 5, 2018

REQUEST FOR PROPOSAL

IDENTITY SERVICES SYSTEM; AND CAMPUS ID/CREDENTIAL MANAGEMENT AND BADGING; AND CAMPUS TRANSACTION SERVICES

RFP 081901

DUE: 3:00 P.M., MST, 12/06/18

Time and Date of Pre-Proposal Conference	11:00 A.M., MST, 11/08/18
Deadline for Inquiries	3:00 P.M., MST, 11/15/18
Time and Date Set for Closing	3:00 P.M., MST, 12/06/18

TABLE OF CONTENTS

TITLE   **PAGE**

EXHIBIT A-   ASU SUN CARD

EXHIBIT B – ASU GUEST CONFERENCE CARD

EXHIBIT C – ASU PROHIBIT SUN CARD

EXHIBIT D-   POS EQUIPMENT

SECTION I – REQUEST FOR PROPOSAL

RFP 081901

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Identity Services System; and Campus ID/Credential Management and Badging; and Campus Transaction Services.** Proposals are to be addressed and delivered to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, (located on the east side of Rural Road between Apache Boulevard and Broadway Road) Tempe, Arizona 85281 **on or before 3:00 P.M. on Thursday, December 6, 2018. No proposal will be accepted after this time. PROPOSALS MUST BE IN A MARKED SEALED CONTAINER** (i.e., envelope, box):

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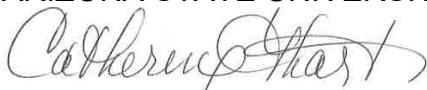RFP Number
Date and Time Proposal is Due

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

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

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

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

ARIZONA STATE UNIVERSITY

_____
Catherine Thart, C.P.M., Purchasing Manager
CT/kd

SECTION II - PURPOSE OF THE RFP

1.   <u>INTENT</u>

Arizona State University ("ASU") wishes to move into a more efficient and futuristic way to deliver solutions for services traditionally used by campus card offices and campus auxiliary services and seeks to engage providers in potential possibilities. The vision is to enhance and streamline the way in which we consume, then provision, distribute, and administer services tied to campus identities; implementing the solutions in a phased approach with each solution choreographed to ensure continuity and a holistic approach.

Beginning with a plan to move from traditional custom "black box" integrations between disparate systems, ASU envisions a central repository of campus community students, staff, faculty and affiliates that are derived from the ASU master identity and access management (IAM) system. Common campus services such as meal board plans and declining balance stored value account management, physical building access, and other services will be downstream beneficiaries within the holistic solution, whereas campus ID card production and mobile credential managed services should have the upstream seamless connectivity with badging software, printing and encoding, and mobile ID credentialing.

In essence the envisioned process and resulting solutions will assemble and conjoin for a holistic approach following the below phases in Figure 1.

We expect the timeline will allow for awards in early 2019 with immediate implementations of the Identify Services (A) and Transaction Services (B) for the Fall semester followed by the other solutions shortly after.

Figure 1

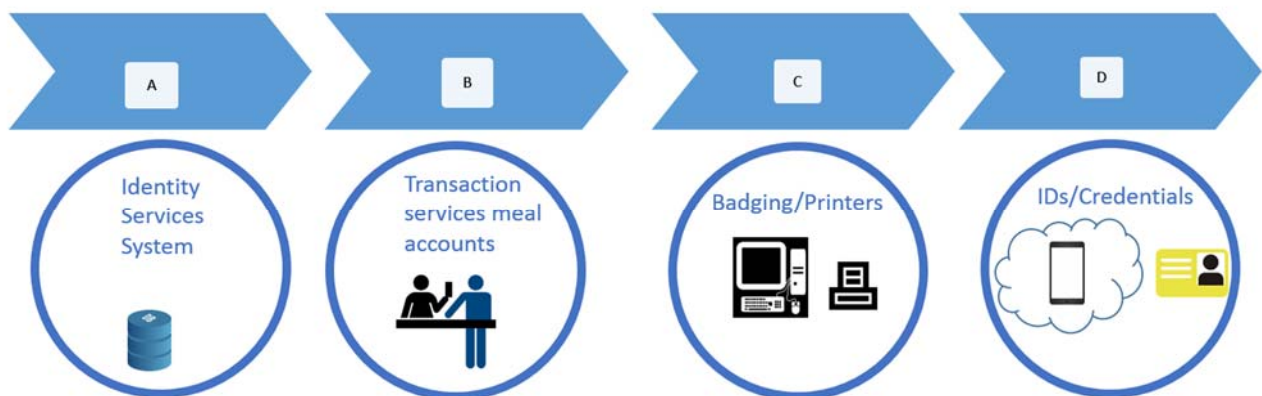Each proposer should exhibit advanced and innovative strategies, and commit to help plan and invest in ASU's future to shape and integrate the futuristic vision that will facilitate ASU's mission to be the leader in a smart campus environment and deliver campus auxiliary services. We expect the provider to bring technical and management expertise to plan and build a new ecosystem intended to enhance campus identity

services to downstream recipients; provide consumables and credential management methodologies; and provide campus transaction services for meal accounts within a traditional auxiliary services program. The proposer's ability to bring technology to expand to mobile use of systems and devices, leverage the emerging Internet of Things (IoT), bring holistic solutions, and sustain ASU's leadership and innovative competitiveness is key to a successful award.

The successful proposer will be required to provide new solutions as well as manage and upgrade the existing equipment, software and related services. It is expected that the successful proposer will show how they will meet the objectives of the section(s) being proposed, meet the specifications, provide competitive pricing within their proposed solution, and bring extended quantity discounts for advancing ASU in both secure mobile credentials and the current ASU physical ID cards. All pricing should be accompanied by a methodology that considers growth and that is dynamic in approach. The successful proposer will show a commitment to invest in the overall strategy to streamline and transform services delivered from ASU's Auxiliary Business Services program. Guidelines and specifications are provided below in the Scope of Work and Attachments.

This RFP is organized into functional areas. Respondents may propose solutions for any portion of this RFP, up to the entire scope of work. As it is understood that suppliers may not be able to effectively provide best-in-class services in every category, the vision is for a holistic approach and it is essential that respondents consider strategies that advance their core area(s) of expertise as well as how they might align with other providers to ensure success. The Scope of Work provides the objectives for each of the following areas of this proposal and Attachments 1, 2 and 3 are intended for proposers to actually respond for one or more of the areas:

Functional Areas in Scope:
    A) Identity Services System
    B) Transactional Services (meal board plan/stored value account services)
    C) Badging Software/Badging Printers
    D) IDs/Mobile Credentials (ID cards and mobile keys/credentials/ credential vault)
    E) Other Value-Add

ASU intends to award one or more contracts to providers under this RFP, but reserves the right to not award any given section if responses do not meet ASU's needs. ASU intends to extend services to other entities either currently or potentially affiliated with ASU in delivery of campus business and auxiliary services and the ASU Enterprise (depicted below) and it is essential that the awarded suppliers be prepared to work closely with these entities. In particular RFP 671292-19ANT - Identity Management Modernization (IMM) Request for Proposal (RFP), to design and build its next generation identity and access management (IAM) system, as well as 341901 - Integrated Technologies Collaborative to design and build new academic initiatives, commercial partnerships, and regional collaborations are to be considered.

The diagram below in Figure 2 depicts the vision of ASU in streamlining the business operations to deliver campus auxiliary services. The solutions that are shown on the right as "A", "B", "C", and "D" are those that can be considered a part of your proposal which include everything with the exception of the physical access control system known as ISAAC access control. ASU is looking for enhancement of solutions along with a streamlined approach to our business operations and have allowed for proposers to offer other value-add solutions ("E") so long as it meets the needs of the university and fits within a holistic approach.
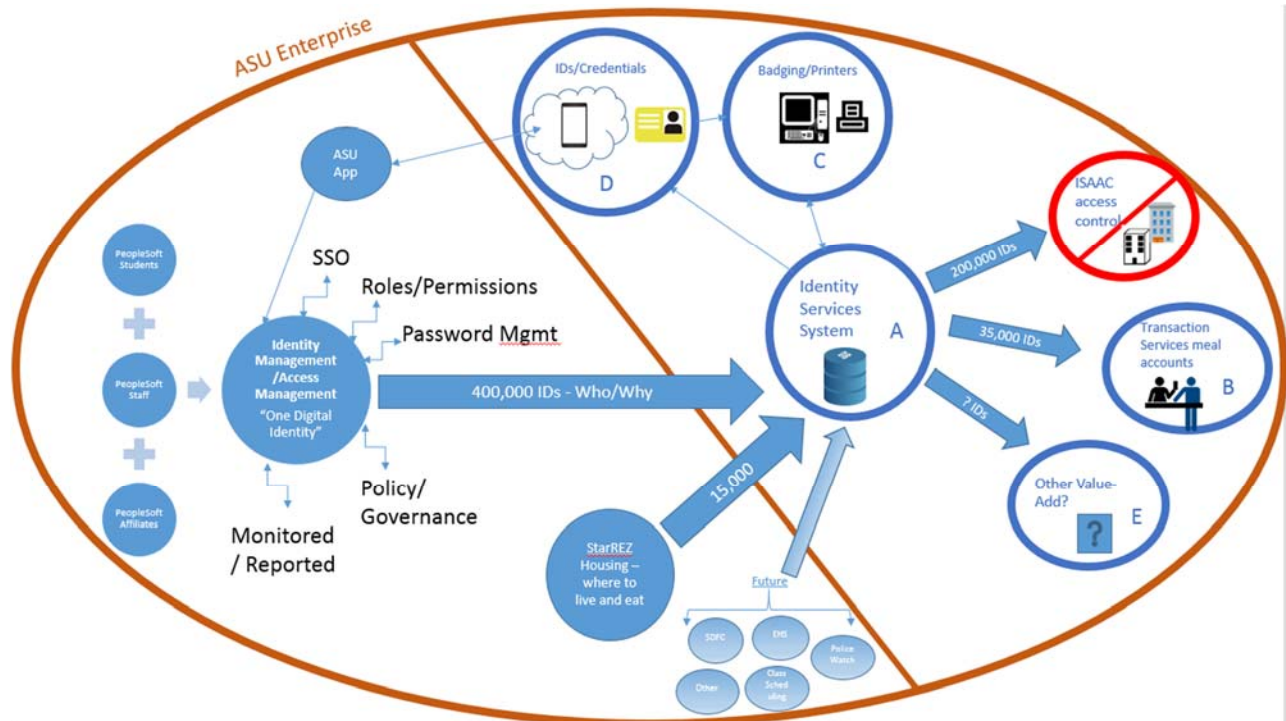

Figure 2

BACKGROUND INFORMATION

ASU has been providing technology-based campus IDs that include both a magnetic stripe and a smart chip since the late 1990s. At this time, ASU has two variations of our card, the basic Sun Card and Pitchfork ID Card, which both utilize HID iCLASS technology. On average, there are approximately 45,000 – 50,000 campus ID cards issued annually and countless visitor/contractor cards used for door access only. ASU has invested into the infrastructure that supports the HID iCLASS technology for door access and will continue to utilize this equipment in conjunction with Lenel OnGuard Pro (known as ISAAC) as the system that supports door access functionality. Currently ASU provides door access credentials at all ASU locations from Washington DC to Santa Monica, California. ASU is open to solutions on expanding into mobile credentials in the use of this current technology across the existing university environment as well as affiliated community platforms outside of just door access. In 2011, in a pilot program [url

below], ASU was notably involved in using mobile phones to open doors and is excited to see this technology leveraged and expanded.

https://www.hidglobal.com/sites/default/files/resource_files/hid-asu-mobile-access-cs-en.pdf

In 2012 ASU entered into a strategic banking partnership with MidFirst Bank and provides services through the issuance our Pitchfork ID Card with Visa® debit card functionality. With the introduction of this card, ASU has stepped away from the use of flexible spending accounts that traditionally funded services such as internal vending, laundry, printing, and an off-campus merchant program. The MidFirst Bank partnership is essential in the campus auxiliary services program and should be carefully considered as an entity to work with to deliver continued services.

Since 2006, ASU has contracted ARAMARK as our food service provider. With this contract, ASU established a mandatory meal plan program for students living in our residential halls. The meal plans vary and are accompanied with alternate accounts, guest meals, meal exchanges, and a declining balance known as Maroon & Gold (M&G) food dollars to be used at ARAMARK locations and at our football stadium, which utilizes Sodexo as their food service provider. With exception of a limited number of Catapult point-of-sale (POS) systems that ARAMARK has provided, ASU provides Micros Simphony POS to ARAMARK to facilitate our meal plan and M&G program. With the Sodexo BuyPass program utilizing their own network, ASU has provided Verifone terminals for M&G in the Stadium. ARAMARK has placed their Catapult system in the markets because of the heavy amount of inventory and run all payment types including credit cards; maintaining their own network and PCI compliance. Other ARAMARK enhanced services include their Campus Dish system for online deposits. ASU currently contracts a service provider, Blackboard, which provides the back-end transactional system that facilitates our meal plan and M&G program. ARAMARK uses this system to manage the meal program and patrons so that they may utilize dining services. ASU is looking for a transaction services meal and stored value system that both ARAMARK and other university departments and partners may use for similar services. ASU expects to maintain our current POS environments. Any transaction meal account solution must be able to transact business with our current POS systems as well as be expandable to other solutions. All PCI must remain out-of-scope for ASU compliance or must meet a strict architecture and information security requirement.

ASU Sun Devil Card Services currently oversees the issuance of all ASU ID cards and verification of identities for photos that will be used across many different university platforms. For card issuance, we have relied on Datacard's IDWorks product. To facilitate the production of the Pitchfork ID card ASU also grants limited access of IDWorks to Midfirst Bank to print the non-banking portion of that card. ASU has historically relied on our transactional system to be the back-end cardholder management system that links to our ID production product. This has

caused unneeded bloat in our current transactional system and we are looking for dedicated identity services solutions to manage identities and associated governance moving forward. Optimally we are also in search of an ID production solution to replace the physical badging solution as well. Over the past 5 years, ASU has created our own photo upload tool and we would like to find additional ways to incorporate this tool into new solutions presented. With the prospect of a new ID production and badging platform ASU is also open to new solutions for ID card printers. In our current environment, ASU is currently utilizing Evolis Primacy printers while Midfirst Bank is using Datacard SD260 printers for ID card production. Current gaps in our operations prohibit the ability to do inline read/encode of our iCLASS credential causing inefficiencies that ASU is looking to providers to propose solutions to close this gap. With the adoption of mobile, ASU looks to provision mobile credentials yet maintain physical card credentials for the near future.

Innovation is at the heart of Arizona State University's plans to extend, expand and reimagine its identity management services for students, faculty, researchers, and staff, as well as to the surrounding community.

"For the fourth year in a row, Arizona State University tops the list of *most innovative schools* in the nation, recognizing the university's groundbreaking initiatives, partnerships, programs and research." [US News and World Report, 2018]

As a national leader and collaborator with Arizona's other public universities, ASU is also publicly soliciting vendors to participate in two other RFPs: 671292-19ANT - Identity Management Modernization (IMM) Request for Proposal (RFP), to design and build its next generation identity and access management (IAM) system, as well as 341901 - Integrated Technologies Collaborative to design and build new academic initiatives, commercial partnerships, and regional collaborations.

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.

ASU has locations across the nation and provides auxiliary services to each and every location including:
- ASU Tempe
- ASU Downtown

- ASU Thunderbird Global Management Downtown
- ASU Polytechnic
- ASU West
- ASU SkySong
- ASU Lake Havasu
- ASU Research Park
- ASU Santa Monica
- ASU Washington DC
- ASU China

If you would like more information about ASU, please visit us at http://www.asu.edu.

2. **TERM OF CONTRACT**

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

The University may consider alternative contract term periods if it is deemed advantageous to do so. If alternative contract terms are proposed, they should be specified in the Pricing Schedule (Attachment 3). 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 <u>Thursday, November 08, 2018</u> at 11am. Attendance will be via a Zoom Video Conference.

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

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

1. **Register by 5:00 p.m. on Wednesday, November 07, 2018**, for the event by sending an email of participants to <u>Catherine.thart@asu.edu</u>. 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 emailed a link and a passcode to enter the online room.

SECTION IV – INSTRUCTIONS TO PROPOSERS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13. **EXCEPTIONS:** The Arizona State University contract terms and conditions are included in this Request for Proposal in Section XII. These terms and conditions will be incorporated into the contract between the University and the successful proposer. **Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed nonresponsive and may be rejected.** All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal. In no event is a Proposer to submit its own standard contract terms and conditions as a response to this RFP.

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

15. Days: Calendar days

    May: Indicates something that is not mandatory but permissible/ desirable.

    Shall, Must, Will: Indicates mandatory requirement. Failure to meet these mandatory requirements will result in rejection of your proposal as non-responsive.

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

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

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

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

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

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

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

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

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

Tel: 480-727-5177
E-mail: Catherine.thart@asu.edu

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

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

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

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

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

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

27. To the extent applicable to any contract resulting from this Request for Proposal, the proposer shall comply with the Standards for Privacy of Individually Identifiable Information under the Health Insurance Portability and Accountability Act of 1996 contained in 45 CFR Parts 160 and 164 (the "HIPAA Privacy Standards") as of the effective date of the HIPAA Privacy Standards on April 14, 2003 or as later determined. Proposer will use all security and privacy safeguards necessary to protect Protected Health Information (PHI), as defined by HIPAA, and shall immediately report to University all improper use or disclosure of PHI of which it becomes aware.

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

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

    Protests should be directed to:

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

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

SECTION V – SPECIFICATIONS/SCOPE OF WORK

The following areas of this scope provide the functional areas on which ASU expects the proposals to satisfy in part or in whole. Each functional area provides information on the expectations for that area and requires the proposer to provide their responses using **Attachment 1, Attachment 2, and Attachment 3.**

Proposers shall demonstrate their ability to fulfill the scope of one or all of these services by providing the responses for each area in the appropriate sections of **Attachment 1, 2 and 3**.

All awarded proposers should be expected to comply with ASU's data governance and information security standards and policies. All software and hardware must be reviewed for compliance to these standards and ASU has the right to reject a proposer who cannot or will not comply with these standards and policies. See Section XIV for more information.

Functional Areas Scope:
This section provides the scope for each of the following areas of this proposal. **Proposers should review this section for Functional Areas Scope but MUST respond to the details surrounding the scope in the list of questions in Attachment 1.** Any section of **Attachment 1** that you are not proposing as a part of your responses to this RFP will require you to indicate an "N" in Column B (Proposal Includes? (Y/N)).

Failure to include your responses in **Attachment 1** may be grounds for rejection of your proposal

A) Identity Services System
ASU envisions a single central repository system of campus community students, staff, faculty and affiliates that will allow us to mitigate risk as well as increase automation as well as gain efficiencies and compliance in our ability to provision identities and provide auxiliary services.

A proposed identity services system should meet the following objectives:

Objectives:
1. Consume the ASU digital identity and affiliated status and roles from the ASU system of source
2. Allow for APIs to other central identity and auxiliary services systems and databases
3. Integrate or allow for APIs with badging software and mobile ID credential vaults to receive badging data and protect it at rest and in transit to other downstream applications.
4. Integrate with various applications to receive policy, permissions, privilege assignments, or affiliated data for workflow approvals
5. Distribute appropriate identities and privileges to multiple downstream beneficiaries with priority on physical access systems and transactions services meal accounts systems
6. Automate approvals through approval workflow and report on exceptions
7. Provide a validation and approval processes that trigger assignment/de-assignment of physical access control for buildings and space
8. Provide a web and mobile end-user self-service function integrated to single-sign-on or an API for use to allow ASU application development for a single ASU experience

9. Provide self-service or visitor service functionality for distribution and provisioning of physical access control assignments and expirations
10. Provide increased visibility of roles, permissions, privileges and approvals given to end-users with authorized levels of reporting and view only capabilities
11. Provide standard detailed reports for business purposes and to comply with FERPA and GDPR as well as standard business intelligence that might interpret behavior, non-compliance of internal controls, or life-cycle management and anomaly control with appropriate reporting.
12. Provide standard exception notifications or alerts sent via email, text, or other protocols and trend or high/low reports of such exception processing
13. Protect personally identifiable information including person and photo as well as encryption keys, system accounts, and credentials or associated data.
14. Provide future proofing methodologies and scalability to provide automated functions and enforcement/notifications via applied rules and policies with other programs
15. Provide continued planning, management, and services to ensure ASU remains a leader in innovation by bringing technological advances forward.
16. Provide standard dashboard views for senior leadership or for public consumption as well as tools (including exporting data) for performing ad-hoc data analysis, data management, and archiving/removal.
17. Provide branding flexibility and ability to customize to ASU branding standards (see https://brandguide.asu.edu/)
18. Optional: expanded services that meet the scope of providing auxiliary services within the holistic vision if based on proposed value-add solutions which may be negotiated at a later time to the awarded proposer

Integrations/System Requirements:

The ability for seamless integrations means that ASU expects certified APIs are already established with multiple vendor applications and that proposers will be able to fulfill the scope depicted in Figure 2 above.

1. Provide details in Attachment 1 for APIs and integrations across the ASU Enterprise ecosystem.
2. Provide details in Attachment 1 for APIs and integrations between Area A and the identified Area B beneficiaries.
3. Provide details in Attachment 1 for APIs and integrations between Area A and the identified upstream Areas C/D.
4. Provide details in Attachment 1 for APIs and integrations between Area A and any identified value-add in Area E.

ASU's technology strategy around system architecture and system requirements is to take advantage of the best of web, mobile and cloud as well as best practice for what is best to remain on-premises.

1. Provide details in Attachment 1 on your system requirements and strategy.
2. Provide details in Attachment 1 on cloud-hosted thresholds and communications.

Considerations:
Considerations of APIs and/or associated SDKs with the following areas is essential to ASU:

1. Identity and Access Management (IAM) - ASU intends to be able to use a best in class IAM across the ASU Enterprise. This IAM is to be yet determined but will be a critical component for planning of the holistic solution (RFP 671292-19ANT)
   o Average estimated active identities consumed for auxiliary services = 226,000
     - Students total 180,000
     - Employees (Faculty Staff) = 20,000
     - Affiliates/Contractors = 15,000
     - Conferees = 10,000
     - Other – 1,000
2. Physical access control – ASU will continue to use the Lenel OnGuard Pro for physical security building and space access as well as intrusion and duress alarm management as a part of this holistic solution
   o Average estimated active credentials = 211,000
     - Students total = 170,000
     - Employees (Faculty/Staff) = 15,000
     - Affiliates/Contractors = 15,000
     - Conferees = 10,000
     - Other – 1,000
3. Transact system meal plan & stored value account – ASU intends to be able to use a meal plan and declining balance system as a part of this holistic solution
   o Average estimated active credentials for meal accounts = 35,000
     - Students total = 30,000
     - Employees (Faculty/Staff) = 2,000
     - Conferees = 2,000
     - Food Service employees = 1,000
4. HID or ASU owned Mobile keys and credentials – ASU intends to be able to issue our own mobile keys and credentials as a part of this holistic solution
   o Average estimated active mobile credentials year 1 = 35,000
     - Freshmen Students total = 15,000
     - Upperclass Students total = 15,000
     - Employee total = 5,000
5. Residential Housing assignment/occupancy program – ASU currently uses the StarREZ program for residential hall management
   - Occupancy total = 15,000
6. For future consideration ASU currently works with
   a. Residential housing - StarREZ
   b. Sun Devil Fitness Center – InnoSoft Fusion
   c. Parking and Transit – T2
   d. Environmental Health and Safety – OnSite EHS Assistant
   e. Classroom/Event Scheduling - Ad Astra/Event Management Systems
   f. Police – Tyler Technologies CAD/Dispatch, Adventos Smartforce
   g. Or Others

B) Transactional services meal board plan/stored value account services
ASU, jointly with ARAMARK, currently utilize a transaction services system that facilitates our meal plan program comprised of traditional board meal plans, meal exchanges, guest plans, and declining balance stored value accounts for dining/food services. A proposed transaction

services system should meet the following objectives for streamlining and enhancing the auxiliary services of the university:

Objectives:
  Software:
  1. Allows for standardized general system administration functionality that takes into account roles and permissions for administration by ASU and by our joint providers that embodies self-sufficiency yet segregation.
  2. Allow for integration and established APIs to other central identity and auxiliary services systems and databases
  3. Allows for user defined fields that can be created, tested and controlled within each segmented merchant by appropriate user-roles
  4. Configurable read/write/modify settings per field by role.
  5. Allows for automated assignment of meal plan and declining balance accounts from upstream integrations.
  6. Works with standard single-sign-on and user management for timeouts, expiration, and multiple login session configuration settings
  7. Allow multiple sessions of the same user to perform administrative functions on the same workstation or multiple workstations and mobile devices at the same time
  8. Ability to add, remove, and modify patrons, plans, hierarchy, accounts, locations, and manage archiving and system logs without negative impacts to the integrity of the system.
  9. Unlimited scalability to grow any standard function of transaction meal account system use
  10. Mobile friendly and agnostic to browsers and PC operating systems
  11. Allows for role-based user initiated bulk import tools, scheduling tools, calendar tools, trial or testing functionality to allow transactions to be completed at location without impacting live reconciliations.
  12. Allows for automated bulk import tools, automated bulk removal of data (account holders, accounts, meal plans, etc), automated account transaction tools, scheduled activities and events, scheduled import/export processes, reconciliation tools, along with ability to perform a trial/test run of tools to determine results without impacts system, and tools for posting and reconciling stored transactions for offline events with ability to restore seamlessly.

  Reporting/Exporting
  13. Provide standard reports in summary and in detail based on merchant, revenue center, revenue center groups, accounts, account types, transaction dates, post dates, identified patron, patron groups, user defined fields, and more.
  14. Provide standard reconciliation reports that can be saved, customized and re-saved or exported for day/time, period, week, month, quarter and annual or calendar-based financials
  15. Provide the ability to create report templates, share report templates, schedule reports, create ad-hoc reports and/or create reports offline to be saved and moved into reporting tool.
  16. Provide the ability to export data in multiple formats with or without headers and line breaks, as well as schedule routine data exports, and email reports or exported data.
  17. Reports for error logs and audit logs of users, system tools, services, workstations, workstation operators, and general financial history.

Meal Accounts Management

18. Provide functionality to allow for internal adjustments from back office workstations that are posted to revenue centers
19. Provide functionality to the food service providers for account-holder balance lookup, transaction detail, combined account aggregation of balances that roll to other accounts as well as separated
20. Access for food service providers to perform uploads of files and data to use with upload tools.
21. Manage accounts, activities, calendars, time-schedules and keyboards per period, expirations, resets based on date or rule, usage policy, or other.
22. Manage behavior and use of meals/accounts based on calendar events, restrict use of an activity to specific days of the week and/or times of the day, set start and end dates for when an activity or account can be used, notify patrons of low balances, notify patrons of food and nutritional choices, notify patrons of location closures or special events like discounts or daily specials, and messages patrons should take action on
23. Manage modifications to accounts that seamlessly incorporate across all account-holders without negative impact.

Patron Management

24. Provide seamless integrations and APIs with other campus systems and current ASU applications for a single ASU experience for our patrons
25. Management of patrons, patron state/status, patron credential/credential state, user-defined-fields, and messages to patrons.
26. Self-service access by patrons for the ability to see balances, show transaction history, maintain active/inactive status of their account, provide online deposits, create guest account access, update personal preferences, keep track of nutritional data, create favorite food choices or locations, and request and save orders
27. Provide patrons multiple options including cash, check, split, campus debit, meal plans, guest plans, cash equivalency, meal exchanges and credit cards and e-wallet.

Merchant/Revenue Center/Device/Location Management

28. Solution must be able to transact business with our current Micros Simphony, Catapult, and ByPass POS systems as well as be expandable to other solutions.
29. Allow for the ability to configure workstations, IP devices, merchant segmentation, revenue centers, accounts, activities, calendars, time-schedules and keyboards per period, expirations, resets based on date or rule, usage policy, roles, Management of tenders, merchants, groups, revenue centers, hierarchy of permissions, cross merchant account types, internal adjustments by patron, or by account type or by group or by revenue center or by merchant
30. Allow for moving devices, locations and groups between revenue centers and merchants without impacting the integrity of the system
31. Allow for devices status to be active or inactive and in a test/training mode
32. Allow for reporting of configurations for locations, devices, tenders, periods, policy, hierarchy, device status

Implementation, Deployment, Training and Support

33. Provide up-front implementation, training, support and system deployment during a typical school out-of-session timeframe or during an in-session timeframe in a manner that will not impact in-session activities

34. Provide on-going implementation, training, support and system deployment, as well as easy to access user interface training methods that are turnkey with no need for administrative burden
35. Provide data migration tools and details on what data can be migrated versus what data cannot be migrated as well as what data can be automated through integration and what data cannot be automated
36. Provide published best practice strategies, trending reports, use cases, knowledge base articles, troubleshooting tips, how-to-guides, release notes, and notifications for system upgrades or system impacts
37. Provide access to software updates, hardware, software and training/installation documentation, remote/regional, or classroom training, technical support and live chat and phone support, and member community via a end-user portal

Security
39. Provide standard detailed reports for business purposes and to comply with FERPA and GDPR as well as standard business intelligence that might interpret behavior, non-compliance of internal controls, or life-cycle management and anomaly control with appropriate reporting.
40. Provide standard exception notifications or alerts sent via email, text, or other protocols and trend or high/low reports of such exception processing
41. Protect personally identifiable information including person and photo as well as encryption keys, system accounts, and credentials or associated data.
42. All PCI must remain out-of-scope for ASU compliance or must meet a strict architecture and information security requirement

Other
43. Provide future proofing methodologies and scalability to provide automated functions and enforcement/notifications via applied rules and policies with other programs
44. Provide continued planning, management, and services to ensure ASU remains a leader in innovation by bringing technological advances forward.
45. Provide standard dashboard views for senior leadership or for public consumption as well as tools (including exporting data) for performing ad-hoc data analysis, data management, and archiving/removal.
46. Provide branding flexibility and ability to customize to ASU branding standards (see https://brandguide.asu.edu/)
47. Optional: buy-out or replacement plan of POS equipment if based on proposed value-add solutions which may be negotiated at a later time to the awarded proposer.
48. Optional: expanded services that meet the scope of providing auxiliary services within the holistic vision if based on proposed value-add solutions which may be negotiated at a later time to the awarded proposer

Integrations/System Requirements:
The ability for seamless integrations means that ASU expects certified APIs that are already established with multiple vendor applications and that proposers will be able to fulfill the scope depicted in Figure 2 above.

1. Provide details in Attachment 1 for APIs and integrations between Area B and the identified Area A.
2. Provide details in Attachment 1 for APIs and integrations between Area B and the identified upstream Areas C/D.

3. Provide details in Attachment 1 for APIs and integrations between Area B and any identified value-add in Area E.

ASU's technology strategy around system architecture and system requirements is to take advantage of the best of both web and cloud as well as equipment and that is best to remain on-premises.

3. Provide details in Attachment 1 on your system requirements and strategy.
4. Provide details in Attachment 1 on cloud-hosted thresholds and communications.

Considerations:
1. POS infrastructure technology – ASU intends to be able to utilize all existing point-of-sale technologies that make up our infrastructure (see EXHIBIT D-POS Equipment).
   o Micros Workstations = 100
   o Catapult Workstations = 20
   o ByPass Workstations = 200
   o Other Point-of-Sale = 40
     ▪ Verifone
     ▪ Freedom Pay
     ▪ Other
2. Board Meal Plans, Guest Plans, Meal Exchanges – ASU intends to be able to continue offering the same or expanded level of traditional meals to students, staff, affiliates and conferees
   o Board/Guest/Exchange Meal Plans = 165 Meal Plans on 13,000 total users
     • Non-Billable University Housing Meal Plans = 450 total users
     • Resident Mandatory Meal Plans = 11,000 total users
     • Non-Resident Meal Plans = 2,000 total users
   o Stored value declining balance accounts = 97 Accounts on 28,000 total users
     • Maroon & Gold traditional account = 6,000 total users
     • Conference account = 6,000
     • Voucher Program account = 16,000 total users
     • ARAMARK Employee account = 1,500 total users
     • Bonus Customer Incentive account = 5,000 total users
3. Multiple Merchants, revenue centers, and grouping – ASU intends to be able to continue offering the same or expanded segregation with multiple ASU Merchants
   o Merchants = 4
     • ARAMARK
     • Athletics/Sodexo
     • Card Office
     • Other Departments
   o Revenue Centers = 103
     • ARAMARK = 100
     • Athletics = 2
     • Card Office = 1
     • Other Departments = TBD

C) Badging software/Badging printers

ASU Sun Devil Card Services currently oversees the issuance of all ASU ID cards and verification of identities for photos that will be used across many different university platforms. The business operations provide a support mechanism and relationship with MidFirst Bank that is paramount for the issuance of Pitchfork IDs. For card issuance, we have relied on Datacard's IDWorks product, which is currently at end of life. A proposed badging software and printer system should meet the following objectives for streamlining and enhancing the auxiliary services of the university:

Objectives:
1. Provide ID badging software/system and printers that use most common industry standard components.
2. Allow for integration and established APIs to other central identity and auxiliary services systems and databases and link card design to any database in real-time
3. Allow for integration or APIs to ASU applications with priority on MyASU, ASU Mobile, ASU Photo upload tool, and other ASU applications
4. Mobile friendly and browser agnostic or allows for PC operating system Windows 7 or higher
5. Allows for unlimited concurrent users and integration to single-sign on
6. Ability for standard administrator functionality for unlimited template design creation, password protect design files, central management and updates of templates across locations and users, creation of user defined fields with configurable read/write and identification of mandatory fields, create users with roles and permissions,
7. Ability for standard crop and adjustment of photos, image and signiture capture, conditionally prints card design elements based on dynamic record values, filter, format and preview record information before printing, and perform search, update, and save of records without printing.
8. Ability to configure and perform logic functions based on fields such as allowance/restrictions on print/save actions
9. Handle the read/write of cards with magnetic stripes and smart chip technologies with primary support of HID iCLASS/SEOS technology
10. Support entries of cardholder information and importing digitized images
11. Standard reports on statistics, volume, daily issuance list with filters by cardholder fields, device, user or location and ability to export or schedule reports for export or email.
12. Enhanced security to prohibit unauthorized shared use, unauthorized print to unauthorized printers, protection of personal information, use of hidden fields, and a detailed and easy to access user audit trail
13. Ability to integrate with multiple industry standard printers with priority on Evolis Primacy and Datacard SD260.
14. Ability to meet the threshold and technical specifications for:
    a. Direct-to-Card
    b. 300 dpi resolution
    c. Print speed should be less than 20 seconds per card for YMCKO single sided printing
    d. Edge to edge printing
    e. Single and dual sided printing capabilities
    f. Offer half panel YMCKO ribbons

g. Provide graphical display on printer with printer menu, ribbon and card consumable status, maintenance, calibration, and software, firmware or other updates
h. Magnetic stripe encoder
i. Proof of support for reading and encoding smart card technologies with priority support for HID iCLASS/SEOS cards with proven integration into ID production software
j. USB and ethernet interface

15. Provide up-front implementation, training, support and system deployment during a typical school out-of-session timeframe or during an in-session timeframe in a manner that will not impact in-session activities.
16. Provide on-going hardware, software, and consumables support, calibration services, hardware warranties, authorized service and repair, returns/hot-swaps, and credits as well as easy to access user interface training methods that are turnkey with no need for administrative burden.
17. Protect personally identifiable information including person and photo as well as encryption keys, system accounts, and credentials or associated data.
18. Provide future proofing methodologies and scalability.
19. Provide continued planning, management, and services to ensure ASU remains a leader in innovation by bringing technological advances forward.
20. Provide branding flexibility and ability to customize to ASU branding standards (see https://brandguide.asu.edu/)
21. Optional: Provide for a hardware leasing agreement opportunity rather than capital expenditures for equipment or a buy-out or cost-effective replacement plan
22. Optional: expanded services that meet the scope of providing auxiliary services within the holistic vision if based on proposed value-add solutions which may be negotiated at a later time to the awarded proposer

Integrations/System Requirements:

The ability for seamless integrations means that ASU expects certified APIs are already established with multiple vendor applications and that proposers will be able to fulfill the scope depicted in Figure 2 above.

1. Provide details in Attachment 1 for APIs and integrations between Area C and the identified Area A.
2. Provide details in Attachment 1 for APIs and integrations between Area C and the identified upstream Areas D.
3. Provide details in Attachment 1 for APIs and integrations between Area C and any identified value-add in Area E.

ASU's technology strategy around system architecture and system requirements is to take advantage of the best of both web and cloud as well as on-prem equipment where it makes sense.

5. Provide details in Attachment 1 on your system requirements and strategy.
6. Provide details in Attachment 1 on cloud-hosted thresholds and communications.

Considerations:

1. Carding technology infrastructure – ASU is looking for proven technology solutions but reserves the right to remain with the current printing platform and/or use some but not all of the current devices all less than 6 years old.
   - Evolis Primacy Printers = 11
   - Datacard SD260 Printers = 10
   - ID Production Stations running Windows 7/10 and IDWorks 6.5 = 19
   - Approximate active users with permission to print cards = 45-50
   - Canon Powershot SX410 IS Cameras = 10
   - Topaz SignatureGem LCD 1x5 Signature Pad = 3

D) ID/Credential Management (ID cards and mobile keys/credentials/credential vault)

ASU provides technology-based campus IDs that include both a magnetic stripe and the HID iCLASS a smart chip. ASU is open to solutions on expanding into mobile credentials in the use of this current technology across existing university as well as affiliated community platforms outside of just door access. The mobile-enabled readers will be either NFC or BLE (blue tooth low energy) and primarily be used first in the physical access control system known as ISAAC on HID/ASSA ABLOY readers. ASU is currently looking for our own mobile key and extended quantity discount pricing on cardstock and credentials:

Objectives:
1. Provide extended quantity discount pricing and production ready ID Cards/Cardstock according to the specifications and artwork in EXHIBIT "A" through "C".
2. Provide the ability to establish a mobile key exclusive to ASU and manage ASU owned credential keys and obtain mobile credentials for use on mobile devices of both iOS and Android
3. Allow for integration and APIs to other central identity and auxiliary services systems and databases
4. Allow administrators to create multiple users and provide roles and permissions in the credential vault
5. The mobile key must be able to securely authenticate on HID/ASSA ABLOY and other mobile-enabled readers
6. Ensure quantity discounts taking into account the total quantity of both card stock and mobile credentials.
7. Provide near 24/7 by 365 credential provisioning to students, faculty, staff and affiliates
8. Provide continued planning, management, and services to ensure ASU remains a leader in innovation by bringing technological advances forward.
9. Provide future proofing methodologies and scalability
10. Provide continued planning, management, and services to ensure ASU remains a leader in innovation by bringing technological advances forward.
10. Provide branding flexibility and ability to customize to ASU branding standards (see https://brandguide.asu.edu/)
11. Optional: expanded services that meet the scope of providing auxiliary services within the holistic vision if based on proposed value-add solutions which may be negotiated at a later time to the awarded proposer

Integrations/System Requirements:

The ability for seamless integrations means that ASU expects certified APIs are already established with multiple vendor applications and that proposers will be able to fulfill the scope depicted in Figure 2 above.

1. Provide details in Attachment 1 for APIs and integrations between Area D and the identified Area C.
2. Provide details in Attachment 1 for APIs and integrations between Area D and the identified upstream Areas A.
3. Provide details in Attachment 1 for APIs and integrations between Area D and any identified value-add in Area E.

ASU's technology strategy around system architecture and system requirements is to take advantage of the best of both web and cloud as well as equipment and that is best to remain on-premises.

4. Provide details in Attachment 1 on your system requirements and strategy.
5. Provide details in Attachment 1 on cloud-hosted thresholds and communications.

Considerations:

a. Current Cardstock Technical Specifications: HID iCLASS SR cards will be pre-programmed using Corporate 1,000 format. Format information will be supplied to awarded supplier. This applies to the ASU Sun Card and Guest Conference cards with iCLASS chip.
b. ASU Sun Devil Card Services annual procurement forecast for each card:
   o ASU Sun Card - Exhibit "A"
      • Estimated purchase = 30,000+ cards annually
   o ASU Guest Conference Card - Exhibit "B"
      • Estimated Procurement = 2,000 cards annually
   o ASU Prohibit Sun Card - Exhibit "C"
      • Estimated procurement = 6,000 cards annually
1. HID or ASU owned Mobile keys and credentials – ASU intends to be able to issue our own mobile keys and credentials as a part of this holistic solution
   o Average estimated active mobile credentials year 1 = 20,000
      • Freshmen Students total = 15,000
      • Employee total = 5,000
2. On delivery of cardstock the terms of sale are F.O.B. Destination. Freight Prepaid via 2-3 day carrier. Title to goods passes to the University at time of delivery and acceptance.
   o ASU will not pay delivery charges.
3. Contractor shall make every endeavor to coordinate delivery schedule of finished product with the ASU Business Service Office. Delivery schedule changes are made by arrangement.
   o Delivery notification shall be made forty-eight (48) hours prior to delivery.
   o Delivery of finished product should be made within seven (7) weeks from the receipt of purchase order.
4. Due to the need for immediate use, the University cannot perform more than a cursory, random inspection. If, as the smart cards are being distributed, errors, or quality problems are discovered, ASU shall have the right, regardless of time of

acceptance or delivery, to demand correction or compensation agreeable to ASU. This correction or compensation may be applied in the form of a credit to future card purchases at ASU's discretion
5. ID Cards and mobile credentials delivered to ASU become the sole property of the University to distribute and dispose of as it deems necessary

E) Value Add

ASU is interested in expanded services that meet the scope of providing auxiliary services within the holistic vision. Industry specific technical and management expertise to plan and build a new ecosystem intended to enhance campus identity services, to bring technology innovation, leverage the emerging Internet of Things (IoT), bring holistic solutions, and sustain ASU's leadership and innovative competitiveness is key to a successful award.

Objectives:
(please detail)

Integrations/System Requirements:
The ability for seamless integrations means that ASU expects certified APIs are already established with multiple vendor applications and that proposers will be able to fulfill the scope depicted in Figure 2 above.

1. Provide details in Attachment 1 for APIs and integrations between Area E and any other area identified in A, B, C or D.

ASU's technology strategy around system architecture and system requirements is to take advantage of the best of both web and cloud as well as equipment and that is best to remain on-premises.

2. Provide details in Attachment 1 on your system requirements and strategy.
3. Provide details in Attachment 1 on cloud-hosted thresholds and communications.

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 in **Attachment 2** may be grounds for rejection of your proposal.

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

2. 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.**

3. All proposals must include information in **Attachment 1 AND Attachment 2 AND Attachment 3** or will be deemed unresponsive. The proposer must indicate on each question in the Attachment 1 whether they are providing a response. For questions that you will not be proposing solutions on please mark each question with an "N" in column B "Proposal Includes? (Y/N)". Please note that information should be addressed on each tab in the spreadsheet.

4. All proposals must include a Pricing Schedule using **Attachment 3**.

5. 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

6. Bidders proposing for D) ID/Credential Management (ID cards and mobile keys/credentials/ credential vault) are required to submit a document with their bid response, from HID Global Corporation as validation of the following mandatory minimum requirements:

    a. Bidder should be an HID Global authorized Value-Added Reseller and an HID Integrator
    b. Bidder should have experience in supplying a minimum of one million (1,000,000) contactless smart cards
    c. Bidder should have no less than five (5) years of experience as an Authorized HID Global Service Provider

7. Provide a detailed overview of the overall management and responsibilities you will provide as well as a sample timeline for implementation.

8. Provide defined standard service level agreements with acceptance of options for additional service-levels agreed upon mutually between proposer and ASU

9. Provide the approach and methodology for system configuration and design, migration of data, go-live support and post launch support, training and user-group/conference opportunities, and on-going collaboration and future-proofing

10. Provide specifications and approach for resources, from all expected participant organizations, that will be necessary for a successful implementation. Include primary and secondary contacts, resumes, org-chart, service standards and escalation model

11. The proposer must provide a minimum of three (3) references with contact information and institution's project launch date and size; a description of a recent project and **proof** of providing services as described in your response portions of this RFP;
    a. References should be verifiable and able to comment on the firm's experience, with a preference for references receiving services similar to those described
    b. Proof should be verifiable through contact references, through on-site presentations and/or pilots, and with transparent and replicable performance by ASU personnel.

SECTION VIII – EVALUATION CRITERIA

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

No.	RFP Criteria Summary	Category %	Evaluation Criteria — Criteria Detail
1	Scope	40%	Response to Section V – Specifications/Scope of Work
2	Qualifications	35%	Response to Section VII - Qualifications
3	Pricing Schedule	15%	Response to Section IX – Pricing Schedule
4	Sustainability	10%	Response to Sustainability Efforts/Sustainability Questionnaire
		100%	

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 using **Attachment 3** to include all aspects of providing the scope of work associated with your responses in this Request for Proposal. Please provide the detailed cost proposal based on the functional area you are proposing and answer any specific cost details in each section you are proposing.

It is important that each submittal include any setup costs, installation costs, implementation fees or other one-time costs, as well as any recurring costs.

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

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.

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

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

Content of Submittal

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

1. Mandatory certifications, Voluntary Product Accessibility Template (VPAT) Sustainability Questionnaire and Substitute W-9 as per Section XIII.

2. Acceptance of ASU's RFP terms and conditions: Note: all exceptions with justification and alternative language MUST be submitted with the proposal.

3. Detailed Response to Specifications/Scope of Work which includes completed Attachment 1 (Supplier Objectives)– Section V

4. Detailed Response to Proposer Qualifications which includes Attachment 2 (Supplier Qualifications)– Section VII

5. Response to Pricing Schedule which includes Attachment 3- Section IX

SECTION XI – PROPOSER INQUIRY FORM

Pre-Proposal Questions, General Clarifications, etc. Email to Catherine.thart@asu.edu.

PROJECT NAME: **Identity Services System; and campus ID/credential management and Badging; and campus transaction services**

PROPOSAL NUMBER: RFP 081901

INQUIRY DEADLINE: 3:00 P.M., MST, November 15, 2018

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

DATE: _____

WRITER: _____

COMPANY: _____

E-MAIL ADDRESS: _____

PHONE: _____   FAX: _____

QUESTIONS:

_____

_____

_____

_____

_____

_____

_____

_____

_____

SECTION XII – AGREEMENT - TERMS & CONDITIONS

The following 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.

Arizona State University Agreement for Identity Services, Campus Credential Management and Campus Transaction System

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 Identity Services, Campus Credential Management and Campus Transaction System 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. This Agreement is effective as of the date of the last signature below (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: 1) 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 two (2) years with the option to renew up to three (3) successive one year Terms. The Term will not exceed 5 years. Following the initial Term, the Agreement may be extended by mutual written agreement.

   b. ASU may terminate the Agreement, with or without cause, upon 30 days written notice to Supplier. 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, 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.

5.   **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, packaging, shipping insurance, and handling; and 3) prices will include any travel, labor, interest, import/export fees, and other costs associated with providing the Goods/Services.

6.   **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.

7.   **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.

8.   **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.

9.   **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 samples furnished by Supplier. In the event of a conflict among the specifications, drawings, samples, and description, the specifications will govern.

10. **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 (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.

11. **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, and all negligent or willful acts or omissions of, Supplier's contractors and subcontractors at all tiers. 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.

12. **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, 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.

13. **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.

14. **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.

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

15. **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, <u>ASU Confidential Information</u>). 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. In addition, 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.

16. **Information Security**. 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); OR 4) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data.

    All systems containing ASU Data must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable laws, rules, and regulations. To diminish information security threats, Supplier will (either directly or through its third party service providers) meet the following requirements:

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

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

    c. <u>Off Shore</u>. Direct Services that may involve access to secure or sensitive ASU Data or personal client data or development or modification of software for ASU, will be performed within the borders of the United States. Unless stated otherwise in the Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of the Agreement. This provision applies to work performed by subcontractors at all tiers and to all ASU Data.

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

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

    f. <u>Notifications</u>. 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 <u>Infosec@asu.edu,</u> in addition to any other notice addresses in the Agreement.

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

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

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

j. Secure Development. Use secure development and coding standards including secure change management procedures in accordance with industry standards. Perform penetration testing and/or scanning prior to releasing new software versions. Supplier will provide internal standards and procedures to ASU for review upon ASU request.

17. **End User Licenses**. The terms of this section apply if the Goods/Services include software or other computer programs or applications that require acceptance of a clickwrap, click-through, end user license, or other similar agreement (End User Agreement) prior to the use of the software. If Supplier requires ASU's individual users to accept an 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 Policy will be null and void.

18. **Background Checks**. 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 those persons employed or contracted by Supplier for security or safety-sensitive positions, as defined in ASU ACD 126, or who may have access to sensitive or highly sensitive ASU data, as defined in ASU's Data Handling Standard. Supplier will conduct all Screenings within 90 days prior to a person commencing work under this Agreement. Supplier will exclude from any direct participation in Supplier's performance under this Agreement any unqualified persons. 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 equal opportunity laws, rules, and regulations.

19. **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.

20. **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.

21. **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.

22. **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.

23. **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.

24. **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.

25. **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.

26. **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.

27. **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.

28. **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.

29. **Force Majeure**. Neither party will be held responsible for any losses resulting if the fulfillment of any terms or provisions of the Agreement are delayed or prevented by any cause not within the control of the party whose performance is interfered with, and which by the exercise of reasonable diligence, the party is unable to prevent. The party impacted by the force majeure will take commercially practicable actions to mitigate the impact of the force majeure.

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; and 3) contingency plans for the Supplier to continue the performance of its obligations under the Agreement, despite the emergency. 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, being obliged to implement the plan is not of itself an occurrence of force majeure, and Supplier will not be entitled to any additional compensation or extension of time by virtue of having to implement it, unless otherwise agreed to by ASU in writing. A Public or Institutional Emergency will mean a natural or manmade 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 or their duly authorized agents.

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. **Labor Disputes**. Supplier will give prompt notice to ASU of any actual or potential labor dispute that delays or may delay performance of the Agreement.

36. **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.

37. **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.

38. **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.

39. **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.

40. **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.

41. **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.

42. **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.

43. **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 any 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.

44. **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.

45. **Essence of Time**. Time will be of the essence as to matters contemplated by the Agreement.

46. **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.**

47. **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.

48. **Arbitration**. The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to ARS § 12-133.

49. **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.

50. **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.

51. **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.

52. **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.

53. **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.

54. **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.

55. **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.

56. **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://www.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.

57. **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. 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.

58. **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.

59. **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.

60. **Tobacco Free**. ASU is tobacco-free. For details visit www.asu.edu/tobaccofree.

61. **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.

62. **No Boycott of Israel**. As 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.

63. **Survival Clause**. 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.

64. **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 below.

65. **Provision of Goods/Services to ASU Related Entities**. ASU has, and expects to enter into additional, service and management contracts with a number of third parties (Related Entities) to deliver some or all of the Goods/Services to ASU students. These Related Entities include, for example, third party managers or owners of ASU student residence halls. At ASU's option, Supplier will provide the Goods/Services to ASU's current and future Related Entities consistent with the terms of the Agreement.

66. **Provision of Good/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 sign a separate Consent and Agreement to be Bound with Supplier, in form and content similar to Exhibit B that so requests. By entering into a Consent and Agreement to be Bound, each Component Unit will agree to be bound by the terms of this Agreement as if it were an original party to the Agreement, and Supplier will agree to provide the Goods/Services directly to the Component Unit. ASU will have no liability or responsibility for the performance of its Component Units under the Consents and Agreements to be Bound. Component Unit means each entity named as a Component Unit in ASU's Comprehensive Annual Financial Report (Note B to Financial Statements). ASU's Component Units are legally separate entities governed by independent boards of directors whose goals are to support ASU or have a close

affiliation with ASU. They are considered part of ASU's knowledge enterprise, but they are not Arizona public bodies, and ASU may not contract on their behalf. ASU's Component Units include the Arizona State University Foundation for a New American University, an Arizona nonprofit corporation, and ASU Preparatory Academy, an Arizona nonprofit corporation. Supplier will enter into a Consent and Agreement to be Bound with each Component Unit that so requests, and, except as may be set forth in the Consent and Agreement to be Bound, Supplier will provide the Goods/Services to such Component Unit to the same extent and on the same terms as if the Component Unit were the customer of the Agreement.

67. **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 31 U.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.

68. **Government Subcontract Provisions**. If this Agreement 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.

    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
52.227-11 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/VFDFARs.htm

69. **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: To Supplier:
Director, Business Applications   _____
University Business Services   _____
Arizona State University   _____
Mailing Address: _____
    PO Box 875212
    Tempe, AZ 85287-5212
Delivery Address:
    1551 S. Rural Rd.
    Tempe, AZ 85287

With a copy to: With a copy to:

Chief Procurement Officer   _____
Purchasing and Business Services   _____
Arizona State University   _____
Mailing Address: _____
    PO Box 875212
    Tempe, AZ 85287-5212
Delivery Address:
    1551 S. Rural Rd.
    Tempe, AZ 85287

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.

70. **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.

71. **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.

72. **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.

73. **State Purchasing Cooperative**. The Agreement and ASU's Identity Services, Campus Credential Management and Campus Transaction System 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.

74. **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:

By:_____

Name:_____

Title:_____

Date Signed:_____

Supplier:

By:_____

Name:_____

Title:_____

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.

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

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

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

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

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

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

c.   Policy will contain a severability of interest provision.

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

a.   Employer's Liability in the amount of $1,000,000 injury and disease.

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

behalf of Supplier.

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

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

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

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

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

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

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

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

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

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

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

**C.	Acceptability of Insurers:** Insurance is to be placed with duly licensed or approved non-admitted 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 <u>Consent</u>) is entered into between _____ (<u>Supplier</u>) and _____, an Arizona nonprofit corporation (<u>Company</u>). This Consent is effective as of the date of the last signature below (the <u>Effective Date</u>).

RECITAL

A.   Effective as of _____, the Arizona Board of Regents for and on behalf of Arizona State University (<u>ASU</u>) and Supplier entered into the Arizona State University Agreement for Background Screening Services (the <u>Agreement</u>) 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 <u>Schedule A</u>.

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.   <u>Consent to be Bound</u>. 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.   <u>Provision of Services</u>. 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.   <u>Company Representations</u>. 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.   <u>Supplier Registrations</u>. 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.   <u>Company Specific Provisions</u>. 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. <u>Other Documents</u>. 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. <u>Further Assurances</u>. 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 is subject to and made in accordance with the Arizona State University Agreement for Identity Services, Campus Credential Management and Campus Transaction System 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
	2 years		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 (<u>SOW</u>) is made in accordance with the Arizona State University Agreement for Identity Services, Campus Credential Management and Campus Transaction System between_____ (<u>Supplier</u>) and the Arizona Board of Regents for and on behalf of Arizona State University (<u>ASU</u>) effective _____ (the <u>Agreement</u>). To the extent any provision in this SOW conflicts with any provision of the Agreement, the provision of the Agreement will control.

EXHIBIT E – SERVICE LEVEL AGREEMENT

This Service Level Agreement (SLA) is made in accordance with the Arizona State University Agreement for Identity Services, Campus Credential Management and Campus Transaction System 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.

SECTION XIII-MANDATORY CERTIFICATIONS

CONFLICT OF INTEREST CERTIFICATION

_____
(Date)

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

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

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

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

_____

_____   _____
(Firm)   (Address)

_____   _____
(Email Address)

_____   _____
(Signature required)   (Phone)

_____   _____
(Print name)   (Fax)

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

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

FEDERAL DEBARRED LIST CERTIFICATION

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

_____
(Date)

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

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

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

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

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

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

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

(2) "Principals," for the purposes of this certification, means officers; directors; owners; partners; and, persons having primary management or supervisory responsibilities within a business entity (_e.g.,_ general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.

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

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

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

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

_____ _____
(Firm) (Address)

_____ _____
(Email Address)

_____ _____
(Signature required) (Phone)

_____ _____
(Print name) (Fax)

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

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

ANTI-LOBBYING CERTIFICATION

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

_____
(Date)

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

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

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

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

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

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

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

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

_____
(Firm)

_____
(Email Address)

_____
(Signature required)

_____
(Print name)

_____
(Print title)

_____
(Address)

_____

_____
(Phone)

_____
(Fax)

_____
(Federal Taxpayer ID Number)

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

LEGAL WORKER CERTIFICATION

_____
(Date)

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

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

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

_____   _____
(Firm)   (Address)

_____   _____
(Email address)

_____   _____
(Signature required)   (Phone)

_____   _____
(Print name)   (Fax)

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

(Purchasing 7/25/16)

Voluntary Product Accessibility Template® (VPAT®)
REVISED SECTION 508 EDITION

Version 2.2
July 2018

ABOUT THIS DOCUMENT

The VPAT is provided in four editions based on the guidelines/standards being evaluated. This is the Revised Section 508 edition of the VPAT. It includes the following standards/guidelines:

- Web Content Accessibility Guidelines 2.0, at *http://www.w3.org/TR/2008/REC-WCAG20-20081211/*

- Revised Section 508 standards as published by the U.S. Access Board in the Federal Register on January 18, 2017, including the Corrections to the ICT Final Rule as published by the US Access Board in the Federal Register on January 22, 2018

If you need a different combination of standards/guidelines then use the appropriate alternate edition of the VPAT found on https://www.itic.org/policy/accessibility/vpat. The choices are WCAG, Revised 508, EN 301 549 and International that includes all three.

This document is broken into two main sections:

- Essential Requirements and Best Practices for using the VPAT® to complete an Accessibility Conformance Report

- The VPAT Template

Please carefully review the Essential Requirements and Best Practices sections before using the VPAT to create an Accessibility Conformance Report. The VPAT 2.2

template includes criteria from WCAG 2.0 and EN 301 549, as well as the Revised Section 508 Standards and Section 255 guidelines.

"Voluntary Product Accessibility Template" and "VPAT," including the template format, are Federally Registered Service Marks of the Information Technology Industry Council (ITI). VPAT 2.2 users agree not to deviate materially from the template format provided by ITI, and to use the service mark ("®") where appropriate.

ESSENTIAL REQUIREMENTS AND BEST PRACTICES FOR INFORMATION & COMMUNICATIONS TECHNOLOGY (ICT) VENDORS

This section provides guidance for reporting product conformance for two major accessibility standards and guidelines using the VPAT® to produce the Accessibility Conformance Report. Deviating from these guidelines precludes vendors from referencing the template by name and/or the VPAT acronym. The purpose of these essential requirements and best practices are to promote accurate and consistent reporting of product accessibility information.

The VPAT is a template used to document a product's conformance with accessibility standards and guidelines. The purpose of the VPAT is to assist customers and buyers in making preliminary assessments regarding the availability of commercial "Electronic and Information Technology," also referred to as "Information and Communication Technology" (ICT) products and services with features that support accessibility.
Getting Started

1. Before creating a report, read all of the materials provided in this document.

2. The Information Technology Industry Council (ITI) provides the VPAT. Use of the template and service mark does not require membership in ITI.

3. Determine which accessibility standards/guidelines will be included in the product conformance report and use the appropriate VPAT file.

4. It is the vendor's responsibility to maintain the integrity of the data in the report.
Essential Requirements for Authors
The following are the minimum requirements to be a VPAT®.

1. The VPAT name and template are registered service marks of ITI. Use of the VPAT template and name requires the inclusion of the registered service mark (i.e., "VPAT®"). Users of the VPAT agree not to deviate from the Essential Requirements for Authors.

2. The template file can be used as is or replicated in a different delivery format, for example as HTML or PDF. The only requirement is that the final conformance report must be accessible.

3. A report may contain a minimum of one applicable Standard/Guideline or any combination of the three Standards/Guidelines that are applicable to the product being reported.

4. A report must contain the following content at a minimum:

   • **Report Title** – In the heading format of "[Company Name] Accessibility Conformance Report"

   • **VPAT Heading Information** – Template version

- **Name of Product/Version** – Name of Product being reported, including version of the product

- **Product Description** – A brief description of the product

- **Date** – Date of report publication. At a minimum, provide the month and year of the report publication. For example, "May 2016". If date is included ensure it is clear "4 May 2016" or "May 4, 2016".

- **Contact Information** – Contact Information for follow-up questions. Listing an email is sufficient.

- **Notes** – Any details or further explanation about the product or the report. This section may be left blank.

- **Evaluation Methods Used** – Include a description of what evaluation methods were used to complete the VPAT for the product under test.

- **Applicable Standards/Guidelines** – A clear indication of which Standards/Guidelines this Conformance Report covers.

  - The list must include only the Standards/Guidelines that were used to develop the product.

  - A report must contain a minimum of one Standard/Guideline or any combination of the three Standards.

  - The applicable Standards/Guidelines that may be included are:

    - Revised Section 508 standards – the U.S. Federal accessibility standard, published by the U.S. Access Board in the Federal Register on January 18, 2017
    - Corrections to the ICT Final Rule – a correction to the Revised Section 508 standards, published by the US Access Board in the Federal Register on January 22, 2018
    - Web Content Accessibility Guidelines 2.0 or WCAG 2.0 (ISO/IEC 40500), at http://www.w3.org/TR/2008/REC-WCAG20-20081211/

  - This information can be in a table format at the top of the report with the table heading 'Standards/Guidelines' and the reported Standards/Guidelines identified.

  - Alternatively, the Standard/Guideline being reported can be clearly identified in the introductory text of the report. If multiple Standards or Guideline tables are included, each table should also be clearly identified as to the Standard or Guideline the criteria that table represents.

- **Terms** – Conformance level terms description section

- **Tables for Each Standard or Guideline** – Tables showing the responses to the criteria.

5. WCAG Conformance Tables – The answers in the WCAG success criteria tables are based on the level of conformance being reported (Level A, AA or AAA).

   o These tables are used to answer:

     ▪ Revised Section 508:
       - Chapter 5 Software
       - Chapter 6 Support Documentation
     ▪ The selected levels of WCAG 2.0 Guidelines.

   o Due to answers applying to multiple criteria, when answering for the Revised Section 508, the answers need to be clear in what individual criteria the answer applies to. It is possible to either use a summary, selecting the worst case for the criteria, or to have separate answers or even tables for software, support documentation, authoring tools, etc., so long as the methodology used is made clear.

6. Conformance Levels – The report must list the definition of the terms used in the Conformance Level column. ITI recommends the following terms. If a vendor deviates from the ITI definitions, the vendor shall reference this change in the heading Notes section. If a term is not used it can be removed from the list. The ITI definitions are:

   - **Supports**: The functionality of the product has at least one method that meets the criterion without known defects or meets with equivalent facilitation.

   - **Partially Supports**: Some functionality of the product does not meet the criterion.

   - **Does Not Support**: The majority of product functionality does not meet the criterion.

   - **Not Applicable**: The criterion is not relevant to the product.

   - **Not Evaluated**: The product has not been evaluated against the criterion. This can only be used in WCAG 2.0 Level AAA.

Note: When filling in the WCAG tables, a response may use 'Supports' where one might otherwise be inclined to use 'Not Applicable'. This is in keeping with WCAG 2.0 Understanding Conformance: 'This means that if there is no content to which a success criterion applies, the success criterion is satisfied.

7. Remarks and Explanations – Detailed remarks should be provided in the Remarks and Explanations column to justify your answer in the Conformance Level column.

- When the conformance level is 'partially supports' or 'does not support', the remarks should identify:

    1. The functions or features with issues

    2. How they do not fully support

- If the criterion does not apply, explain why.

- If an accessible alternative is used, describe it.

8. In the Section 508 tables, when subsections of criteria do not apply to the product, the section may be summarized or removed as long as an explanation is provided explaining why a criterion does not apply. Another alternative is to leave the table and add a summary why the section doesn't apply. For example, in Chapter 5 the criteria in 502 and 503 will not apply to a web only application, thus those sections can be removed with a summary in the notes for the chapter, or a row in the table.

Best Practices for Authors

ITI suggests that authors adopt the following best practices when using the VPAT® to create an Accessibility Conformance Report.

- **Branding Header:** Company logo or branding information

- **Date Changes:** If a report is revised, change the report date and explain the revision in the Notes section. Alternately, create a new report and explain in the Notes section that it supersedes an earlier version of the report.

- **Notes:** Add any notes applicable to product or the report

    - Additional information about the product version that the document references

    - Any revisions to the document

    - Links to any related documents

    - Additional information describing the product

    - Additional information about what the document does or does not cover

    - Information suggested by the WCAG 2.0 Conformance Claim, at http://www.w3.org/TR/WCAG20/#conformance-claims

    - Information needed to satisfy ISO/IEC 17050-1:2004, Supplier's Declaration of Conformity

- **Evaluation Methods Used –** Information to enter may include the following:

- Testing is based on general product knowledge

- Similar to another evaluated product

- Testing with assistive technologies

- Published test method (provide name, publisher, URL link)

- Vendor proprietary test method

- Other test method

- **Remarks and Explanations:** This section may include:

  - Information regarding the testing of a given criteria.

  - Information on application dependencies to support accessibility (e.g. OS, app frameworks, browsers recommended).

  - How the customer can find more information about accessibility issues. One method can be to include the bug ID where customers can call the company's customer support to get additional information.

  - Known workarounds for accessibility issues.

- **Legal Disclaimer:** Area for any legal disclaimer text required by your organization.

- **Saving Space:** To reduce the size of the report it is acceptable to remove sections. Individual criteria cannot be removed, only sections at a time. Section removal is acceptable in four situations:

  - When an entire section is not being reported on because it doesn't apply to the product, for example:

    - Chapter 4: Hardware. Information should be included in the notes for that section why it has been removed.

    - A card reader that doesn't have sound could remove the criteria in section 413 Closed Caption Processing Technologies and just note the why the criteria doesn't apply.

  - If the product is not being evaluated for a level of the criteria (for example Level AAA) then that table may be deleted.

  - If a requesting customer has identified that a section of the standard does not apply, information should be included in the notes that the section has been removed.

- **WCAG 2.0 Tables:** The WCAG 2.0 criteria is shown in three tables, Level A, Level AA, and Level AAA.

  - If desired, these tables can be combined into one table.

- When reporting on a level (A, AA or AAA) all criteria for that level must be answered.

- **Language:** Use text appropriate for your audience.

- **Multiple Reports:** When using the VPAT to create an Accessibility Conformance Report for complex products it may be helpful to separate answers into multiple reports. For example, when a product is an Authoring Tool that also has web content and documentation. When multiple reports are used for a complex product, it is required to explain this and how to reach the other reports in the Notes section of each report.

- **Criteria Text:** To help conserve space in the ITI template only the criteria ID number and a short title have been included. Where possible, links have been included to the standard/guideline.

  - It is acceptable to add the full text of the criteria into the cell if desired to help with understanding.

  - The links to the standards/guidelines can be removed.

- **Ordering of Tables:** The order that the standards/guideline tables appear may be changed to facilitate reading. For example, if the Accessibility Conformance Report is for Section 508 only, the WCAG tables may be moved to follow the numbering scheme used in the Section 508 criteria.

- **Guideline Section Heading Rows in Tables:** The tables include heading rows to facilitate understanding the context of the criteria.

  - The cells in these rows do not require answers as indicated by "Heading cell – no response required."
  - It is optional to add a response if desired.

  - The shading of the row is also optional.

  - If removing the heading rows, edit the criteria titles so it's clear where they apply.

Posting the Final Document

- Remove the *Essential Requirements and Best Practices for Information & Communications Technology (ICT) Vendors* section from the template when publishing your Accessibility Conformance Report in final form. A link on page one in the template footnotes contains a hyperlink to this document on the Information Technology Industry Council (ITI) website at: http://www.itic.org.

- Check for each required item in the VPAT® document:

  - The report title **[Company Name] Accessibility Conformance Report**

  - **The "VPAT® Version 2.2" heading**

- **Name of Product/Version**

- **Product Description**

- **Date**

- **Contact Information**

- **Notes**

- **Evaluation methods used**

- **Applicable Standards/Guidelines**

- **Terms**

- **Report Information**

    - Check that there is a response for each criterion for 'Conformance Level' and 'Remarks and Explanations.'

- Post your final document on your company's web site, or make the document available to customers upon request.

- Your final document should be accessible.

Table Information for VPAT® Readers

For each of the standards, the criteria are listed by chapter in a table. The structures of the tables are: the first column contains the criteria being evaluated, the second column describes the level of conformance of the product regarding the criteria and the third column contains any additional remarks and explanations regarding the product.

- When sections of criteria do not apply, or deemed by the customer as not applicable, the section is noted as such and the rest of that table may be removed for that section.

- When multiple standards are being recorded in this document, the duplicative sections are noted and responded to only one time. The duplicate entry will note the cross reference to the data.

[COMPANY] ACCESSIBILITY CONFORMANCE REPORT REVISED SECTION 508 EDITION

VPAT® **Version 2.2 – July 2018**

Name of Product/Version:
Product Description:
Date:
Contact information:
Notes:
Evaluation Methods Used:
Applicable Standards/Guidelines
This report covers the degree of conformance for the following accessibility standard/guidelines:

Standard/Guideline	Included In Report
Web Content Accessibility Guidelines 2.0, at *http://www.w3.org/TR/2008/REC-WCAG20-20081211/*	Level A (Yes) Level AA (Yes) Level AAA (No)
Revised Section 508 standards as published by the U.S. Access Board in the Federal Register on January 18, 2017 Corrections to the ICT Final Rule as published by the US Access Board in the Federal Register on January 22, 2018	(Yes)

Terms

The terms used in the Conformance Level information are defined as follows:

- **Supports**: The functionality of the product has at least one method that meets the criterion without known defects or meets with equivalent facilitation.
- **Partially Supports**: Some functionality of the product does not meet the criterion.
- **Does Not Support**: The majority of product functionality does not meet the criterion.
- **Not Applicable**: The criterion is not relevant to the product.
- **Not Evaluated**: The product has not been evaluated against the criterion. This can be used only in WCAG 2.0 Level AAA.

WCAG 2.0 Report
Tables 1 and 2 also document conformance with:
- Chapter 5 – 501.1 Scope, 504.2 Content Creation or Editing
- Chapter 6 – 602.3 Electronic Support Documentation

Note: When reporting on conformance with the WCAG 2.0 Success Criteria, they are scoped for full pages, complete processes, and accessibility-supported ways of using technology as documented in the WCAG 2.0 Conformance Requirements.

Table 1: Success Criteria, Level A

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.1.1 Non-text Content (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.2.1 Audio-only and Video-only (Prerecorded) (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.2.2 Captions (Prerecorded) (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.2.3 Audio Description or Media Alternative (Prerecorded) (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.3.1 Info and Relationships (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.3.2 Meaningful Sequence (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:

Criteria	Conformance Level	Remarks and Explanations
1.3.3 Sensory Characteristics (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.4.1 Use of Color (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.4.2 Audio Control (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.1.1 Keyboard (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.1.2 No Keyboard Trap (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.2.1 Timing Adjustable (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.2.2 Pause, Stop, Hide (Level A) Also applies to: • Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:

Criteria	Conformance Level	Remarks and Explanations
2.3.1 Three Flashes or Below Threshold (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.4.1 Bypass Blocks (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) – Does not apply to non-web software • 504.2 (Authoring Tool) • 602.3 (Support Docs) – Does not apply to non-web docs	Web: Electronic Docs: Authoring Tool:	Web: Electronic Docs: Authoring Tool:
2.4.2 Page Titled (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.4.3 Focus Order (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.4.4 Link Purpose (In Context) (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.1.1 Language of Page (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.2.1 On Focus (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:

Criteria	Conformance Level	Remarks and Explanations
• 602.3 (Support Docs)		
3.2.2 On Input (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.3.1 Error Identification (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.3.2 Labels or Instructions (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
4.1.1 Parsing (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
4.1.2 Name, Role, Value (Level A) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:

Table 2: Success Criteria, Level AA

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.2.4 Captions (Live) (Level AA) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.2.5 Audio Description (Prerecorded) (Level AA)	Web: Electronic Docs:	Web: Electronic Docs:

Criteria	Conformance Level	Remarks and Explanations
Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Software: Authoring Tool:	Software: Authoring Tool:
1.4.3 Contrast (Minimum) (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.4.4 Resize text (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
1.4.5 Images of Text (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.4.5 Multiple Ways (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) – Does not apply to non-web software 504.2 (Authoring Tool) 602.3 (Support Docs) – Does not apply to non-web docs	Web: Electronic Docs: Authoring Tool:	Web: Electronic Docs: Authoring Tool:
2.4.6 Headings and Labels (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
2.4.7 Focus Visible (Level AA) Also applies to: Revised Section 508 501 (Web)(Software) 504.2 (Authoring Tool) 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.1.2 Language of Parts (Level AA)	Web:	Web:

Criteria	Conformance Level	Remarks and Explanations
Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Electronic Docs: Software: Authoring Tool:	Electronic Docs: Software: Authoring Tool:
3.2.3 Consistent Navigation (Level AA) Also applies to: Revised Section 508 • 501 (Web)(Software) – Does not apply to non-web software • 504.2 (Authoring Tool) • 602.3 (Support Docs) – Does not apply to non-web docs	Web: Electronic Docs: Authoring Tool:	Web: Electronic Docs: Authoring Tool:
3.2.4 Consistent Identification (Level AA) Also applies to: Revised Section 508 • 501 (Web)(Software) – Does not apply to non-web software • 504.2 (Authoring Tool) • 602.3 (Support Docs) – Does not apply to non-web docs	Web: Electronic Docs: Authoring Tool:	Web: Electronic Docs: Authoring Tool:
3.3.3 Error Suggestion (Level AA) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:
3.3.4 Error Prevention (Legal, Financial, Data) (Level AA) Also applies to: Revised Section 508 • 501 (Web)(Software) • 504.2 (Authoring Tool) • 602.3 (Support Docs)	Web: Electronic Docs: Software: Authoring Tool:	Web: Electronic Docs: Software: Authoring Tool:

Table 3: Success Criteria, Level AAA

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.2.6 Sign Language (Prerecorded) (Level AAA) Also applies to: Revised Section 508 – Does not apply	Web:	Web:

Criteria	Conformance Level	Remarks and Explanations

1.2.7 Extended Audio Description (Prerecorded) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.2.8 Media Alternative (Prerecorded) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.2.9 Audio-only (Live) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.4.6 Contrast Enhanced (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.4.7 Low or No Background Audio (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.4.8 Visual Presentation (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

1.4.9 Images of Text (No Exception) Control (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.1.3 Keyboard (No Exception) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.2.3 No Timing (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.2.4 Interruptions (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.2.5 Re-authenticating (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.3.2 Three Flashes (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.4.8 Location (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

Criteria	Conformance Level	Remarks and Explanations

2.4.9 Link Purpose (Link Only) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

2.4.10 Section Headings (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.1.3 Unusual Words (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.1.4 Abbreviations (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.1.5 Reading Level (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.1.6 Pronunciation (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.2.5 Change on Request (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.3.5 Help (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

3.3.6 Error Prevention (All) (Level AAA)
    Also applies to:
    Revised Section 508 – Does not apply
	Web:	Web:

Revised Section 508 Report
Notes:
Chapter 3: Functional Performance Criteria (FPC)
Notes:

Criteria	Conformance Level	Remarks and Explanations
302.1 Without Vision		
302.2 With Limited Vision		
302.3 Without Perception of Color		
302.4 Without Hearing		
302.5 With Limited Hearing		
302.6 Without Speech		
302.7 With Limited Manipulation		
302.8 With Limited Reach and Strength		
302.9 With Limited Language, Cognitive, and Learning Abilities		

Chapter 4: Hardware
Notes:

Criteria	Conformance Level	Remarks and Explanations
402 Closed Functionality	Heading cell – no response required	Heading cell – no response required
402.1 General	Heading cell – no response required	Heading cell – no response required
402.2 Speech-Output Enabled	Heading cell – no response required	Heading cell – no response required
402.2.1 Information Displayed On-Screen		
402.2.2 Transactional Outputs		
402.2.3 Speech Delivery Type and Coordination		
402.2.4 User Control		
402.2.5 Braille Instructions		
402.3 Volume	Heading cell – no response required	Heading cell – no response required
402.3.1 Private Listening		
402.3.2 Non-private Listening		
402.4 Characters on Display Screens		
402.5 Characters on Variable Message Signs		
403 Biometrics	Heading cell – no response required	Heading cell – no response required
403.1 General		
404 Preservation of Information Provided for Accessibility	Heading cell – no response required	Heading cell – no response required
404.1 General		

Criteria	Conformance Level	Remarks and Explanations
405 Privacy	Heading cell – no response required	Heading cell – no response required
405.1 General		
406 Standard Connections	Heading cell – no response required	Heading cell – no response required
406.1 General		
407 Operable Parts	Heading cell – no response required	Heading cell – no response required
407.2 Contrast		
407.3 Input Controls	Heading cell – no response required	Heading cell – no response required
407.3.1 Tactilely Discernible		
407.3.2 Alphabetic Keys		
407.3.3 Numeric Keys		
407.4 Key Repeat		
407.5 Timed Response		
407.6 Operation		
407.7 Tickets, Fare Cards, and Keycards		
407.8 Reach Height and Depth	Heading cell – no response required	Heading cell – no response required
407.8.1 Vertical Reference Plane		
407.8.1.1 Vertical Plane for Side Reach		
407.8.1.2 Vertical Plane for Forward Reach		
407.8.2 Side Reach		
407.8.2.1 Unobstructed Side Reach		
407.8.2.2 Obstructed Side Reach		
407.8.3 Forward Reach		
407.8.3.1 Unobstructed Forward Reach		
407.8.3.2 Obstructed Forward Reach		
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach		
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach		
408 Display Screens	Heading cell – no response required	Heading cell – no response required
408.2 Visibility		
408.3 Flashing		
409 Status Indicators	Heading cell – no response required	Heading cell – no response required
409.1 General		
410 Color Coding	Heading cell – no response required	Heading cell – no response required

Criteria	Conformance Level	Remarks and Explanations
410.1 General		
411 Audible Signals	Heading cell – no response required	Heading cell – no response required
411.1 General		
412 ICT with Two-Way Voice Communication	Heading cell – no response required	Heading cell – no response required
412.2 Volume Gain	Heading cell – no response required	Heading cell – no response required
412.2.1 Volume Gain for Wireline Telephones		
412.2.2 Volume Gain for Non-Wireline ICT		
412.3 Interference Reduction and Magnetic Coupling	Heading cell – no response required	Heading cell – no response required
412.3.1 Wireless Handsets		
412.3.2 Wireline Handsets		
412.4 Digital Encoding of Speech		
412.5 Real-Time Text Functionality	Reserved for future	Reserved for future
412.6 Caller ID		
412.7 Video Communication		
412.8 Legacy TTY Support	Heading cell – no response required	Heading cell – no response required
412.8.1 TTY Connectability		
412.8.2 Voice and Hearing Carry Over		
412.8.3 Signal Compatibility		
412.8.4 Voice Mail and Other Messaging Systems		
413 Closed Caption Processing Technologies	Heading cell – no response required	Heading cell – no response required
413.1.1 Decoding and Display of Closed Captions		
413.1.2 Pass-Through of Closed Caption Data		
414 Audio Description Processing Technologies	Heading cell – no response required	Heading cell – no response required
414.1.1 Digital Television Tuners		
414.1.2 Other ICT		
415 User Controls for Captions and Audio Descriptions	Heading cell – no response required	Heading cell – no response required
415.1.1 Caption Controls		
415.1.2 Audio Description Controls		

Chapter 5: Software

Notes:

Criteria	Conformance Level	Remarks and Explanations
501.1 Scope – Incorporation of WCAG 2.0 AA	See WCAG 2.0 section	See information in WCAG section
502 Interoperability with Assistive Technology	Heading cell – no response required	Heading cell – no response required
502.2.1 User Control of Accessibility Features		
502.2.2 No Disruption of Accessibility Features		
502.3 Accessibility Services	Heading cell – no response required	Heading cell – no response required
502.3.1 Object Information		
502.3.2 Modification of Object Information		
502.3.3 Row, Column, and Headers		
502.3.4 Values		
502.3.5 Modification of Values		
502.3.6 Label Relationships		
502.3.7 Hierarchical Relationships		
502.3.8 Text		
502.3.9 Modification of Text		
502.3.10 List of Actions		
502.3.11 Actions on Objects		
502.3.12 Focus Cursor		
502.3.13 Modification of Focus Cursor		
502.3.14 Event Notification		
502.4 Platform Accessibility Features		
503 Applications	Heading cell – no response required	Heading cell – no response required
503.2 User Preferences		
503.3 Alternative User Interfaces		
503.4 User Controls for Captions and Audio Description	Heading cell – no response required	Heading cell – no response required
503.4.1 Caption Controls		
503.4.2 Audio Description Controls		
504 Authoring Tools	Heading cell – no response required	Heading cell – no response required
504.2 Content Creation or Editing (if not authoring tool, enter "not applicable")	See WCAG 2.0 section	See information in WCAG section
504.2.1 Preservation of Information Provided for Accessibility in Format Conversion		
504.2.2 PDF Export		
504.3 Prompts		
504.4 Templates		

Chapter 6: Support Documentation and Services

Notes:

Criteria	Conformance Level	Remarks and Explanations
601.1 Scope	Heading cell – no response required	Heading cell – no response required
602 Support Documentation	Heading cell – no response required	Heading cell – no response required
602.2 Accessibility and Compatibility Features		
602.3 Electronic Support Documentation	See [WCAG 2.0](#) section	See information in WCAG section
602.4 Alternate Formats for Non-Electronic Support Documentation		
603 Support Services	Heading cell – no response required	Heading cell – no response required
603.2 Information on Accessibility and Compatibility Features		
603.3 Accommodation of Communication Needs		

Legal Disclaimer (Company)
Include your company legal disclaimer here, if needed

The Supplier Sustainability Questionnaire is used to help the University understand how sustainable a supplier is. Sustainability is an important goal for the University, and as such, we expect our suppliers to help us support this goal.

Sustainability Questionnaire

Internal practices

1) Does your firm have published sustainability goals and a plan? Yes ☐ / No☐
   If so, provide the link:

   > (link)

2) Does your firm have published sustainability progress metrics?   Yes ☐ / No☐
   If so, provide the link:

   > (link)

3) ASU has a goal to achieve carbon neutrality by 2025 for Scope 1 & 2 emissions and by 2035 for Scope 3. Do you have a public carbon neutrality goal?
   If so, provide the link: Yes ☐ / No☐

   > (link)

4) Has your firm conducted a greenhouse gas inventory?   Yes ☐ / No☐
   If so, provide:

	Year	Qty (MTCDE)
Baseline		
Most Recent		
% Increase (decrease) vs baseline		%

   Comments:

   > (comments)

5) Has your firm taken measures to reduce emissions related to air and commuting travel?
   Yes ☐ / No☐

   If yes, please provide some examples:

   > (examples)

6) ASU has a goal to divert 90% of its waste from landfills by 2025. Does your organization have a waste diversion goal?   Yes ☐ / No☐

If so, provide the link.

```
(link)
```

7) Does your firm track its solid waste?   Yes □ / No□

If so, provide the following (indicate units of tons or lbs., as appropriate):

	Year	Recycled	Compost	Landfill
Baseline				
Most Recent				

Comments:

```
(comments)
```

8) Has your firm taken measures to reduce printing and paper waste? Yes □ / No□
   If yes, provide some examples:

```
(examples)
```

9) ASU has a goal to reduce water use by 20% by 2022. Does your organization have a
   water reduction goal?   Yes □ / No□
   If so, provide the link:

```
(link)
```

10) Does your organization participate in / support community service, not-for-profit
    organizations and inclusive community success?   Yes □ / No□

If yes, provide some examples:

```
(examples)
```

11) Has your firm developed measures to improve organizational diversity and inclusion and
    enhance employee engagement?   Yes □ / No□

If yes, provide some examples:

```
(examples)
```

12) Does your company have any external ratings, certifications or awards related to diversity, inclusion and employee engagement? (GPTW, JUST, etc.)

Yes ☐ / No☐

If yes, provide the names and a link:

(name and link of certifications)

13) Does your company have any external sustainability certifications? (DJSI, GRI, GBB, Green C, Certified B Corporation, Green America, Green Plus, etc.)

Yes ☐ / No☐

If yes, provide the names and links:

(name and links of certifications)

14) Has your company committed to any goals created by an external organization related to climate change? Yes ☐ / No☐

If so, provide the goals your company has committed to:

(name and links)

15) Are there any other sustainability efforts you would like to mention?

(Comments)

Financial Services
FATCA Compliant Substitute W-9

ARIZONA STATE UNIVERSITY

RETURN TO ASU		DO NOT SEND TO IRS

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

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

► LEGAL NAME: (must match TIN)	

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

CITY:		ST:		ZIP:	

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

CITY:		ST:		ZIP:	

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

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

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

► CERTIFICATION

Under penalties of perjury, I certify that:

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

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

Signature of U.S. Individual	Date:

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

ASU | ARIZONA STATE UNIVERSITY

Financial Services
Vendor Authorization Form

RETURN TO ASU		DO NOT SEND TO IRS

► **Legal Name:**	**TIN:**

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

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

SECTION 1 - FEDERAL INFORMATION

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

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

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

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

SECTION 2 - STATE OF ARIZONA SMALL BUSINESS INFORMATION

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

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

Print Name:	
Signature:	

Phone:	Fax:

Email:

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

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

SECTION XIV – SECURITY REVIEW PROCESS (REFERENCE DOCUMENT #1)
Form version: 2016-06-20

Expectations

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

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

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

Overview

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

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

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

Scope of Review

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

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

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

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

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

Project Information

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

```
```

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

```
```

This project is not using Planview.

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

```
```

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

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

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

Responsibility for Secure Design

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

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

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

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

Additional information (optional)

Sensitive Data

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

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

Regulated Data
- ☐ PCI regulated (credit card data)
- ☐ FERPA regulated (student data)
- ☐ HIPAA regulated (health data)
- ☐ ITAR (import, export, defense-related technical data or foreign students)

ASU Data Classifications

- ☐ Highly Sensitive - disclosure endangers human life health or safety
- ☐ Sensitive - regulated data (including regulations above) or Personally Identifiable Information
- ☐ Internal - a login is required
- ☐ Public - anyone can see it without logging in

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

```

```

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

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

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

☐	**Unknown**	We haven't determined this yet, for some or all connections.
☐	**High**	Sensitive data will be traveling across one or more connections without any protection.
☐	**High**	All systems and connections storing or processing sensitive data are within the ASU data center, but sensitive data is not encrypted as it moves from system to system.
☐	**High**	Firewalls, network segmentation, and/or other techniques limit sensitive traffic to only those systems that are intended to receive it. Other systems are prevented from connecting, or listening to sensitive traffic. However, sensitive data is not encrypted in transit.
☐	**Addressed**	All sensitive data is encrypted as it travels over each network connection.
☐	**Addressed**	All* web sites are using https encryption. Servers have valid https certificates. (The certificates are correctly configured and installed so that no warnings are seen.)
☐	**Addressed**	This project has no sensitive data.
☐	**Addressed**	This question is not applicable for this project because all of the following are true: ● No ASU equipment or network connections will be used to transmit sensitive data. ● If a vendor is transmitting or receiving sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISOlanguage.

Additional information (optional)

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

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

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

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

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

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

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

Additional information (optional)

Security Architecture Diagram

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

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

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

Has a complete security architecture diagram been submitted?

☐	**Unknown**	The security architecture diagram has not yet been submitted.

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

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

Additional information (optional)

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

Servers

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

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

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

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

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

Production (intended for normal use)

```



```

QA (should be virtually identical to production)

```



```

Development (for unfinished work, programmer testing etc.)

```



```

Additional information (optional)

```



```

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

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

Additional information (optional)

<div style="border:1px solid black; height:100px;"></div>

Web Servers

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

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

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

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

Production (intended for normal use)

<div style="border:1px solid black; height:80px;"></div>

QA (should be virtually identical to production)

<div style="border:1px solid black; height:80px;"></div>

Development (for unfinished work, programmer testing etc.)

<div style="border:1px solid black; height:80px;"></div>

Additional information (optional)

<div style="border:1px solid black; height:80px;"></div>

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

☐	**Unknown**	At present we don't know if there will be development or QA instances of the web site(s).

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

Additional information (optional)

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

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

Additional information (optional)

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

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

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

Additional information (optional)

Database Servers

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

What database protections are in place?

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

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

Additional information (optional)

User Authentication

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

☐	**Unknown** (red)	User authentication systems have not yet been defined.
☐	**High** (red)	When a user logs in, their password is sent across the network without encryption. For example, users log in from a web page that does not use https encryption. Or as another example, users have client software on their computers which logs in to a server, but the connection to the server is not encrypted.
☐	**High** (red)	One or more systems maintain an independent user authentication technique instead of standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
☐	**Medium** (orange)	The login page uses https encryption and standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS, but subsequent pages revert back to http.
☐	**Low** (yellow)	Ordinary users are authenticated using standard ASU enterprise "single-sign-on" systems, but privileged users, such as site owners or administrators, are authenticated using a separate mechanism.
☐	**Addressed** (green)	All systems that require users to identify themselves use standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
☐	**Addressed** (green)	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, <u>both ends of the connection</u> should have a way to verify that the other server is the correct one and not an impostor.

How do the project's servers authenticate each other?

☐	**Unknown**	Server authentication techniques have not yet been defined.
☐	**High**	One or more servers initiate or accept connections with their peers, but do not verify or otherwise restrict which servers can connect.
☐	**High**	When a server logs in to another server, a password or other secret is transmitted across a network connection without encryption.
☐	**Medium**	Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a "black list" identifying which addresses are not allowed to connect.
☐	**Low**	Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a "white list" specifically identifying which addresses are allowed to connect, and denying all others by default.
☐	**Low**	Servers use credentials to identify each other, but there are weaknesses (explain in the notes). For example: (A) the credentials are not unique to one application (B) the credentials are not safely stored, or (C) it is difficult to change the credentials.
☐	**Addressed**	Each server uses a standard mechanism, such as https, to verify the other server's identity when initiating a connection to another server. If using https, servers have valid https certificates, and clients verify certificate validity. (The certificates are correctly configured and installed so that no warnings are seen.) The listening server authenticates the requesting server using credentials that are unique to this application. The credentials are not stored where they can be accessed without authorization. Credentials are periodically updated, and can be quickly updated if a compromise is suspected.
☐	**Addressed**	The project does not have more than one server, so there is no need for servers to authenticate each other.
☐	**Addressed**	The changes being made as part of this project will not affect a situation where two or more servers are communicating with each other, so the question does not apply.

Additional information (optional)

Vendor Involvement

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

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

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

Vendor	Date vendor signed contract with ISO language

Additional information (optional)

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

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

Additional information (optional)

Backup, Disaster Recovery, and Business Continuity Strategy

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

What is the backup strategy?

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

Additional information (optional)

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

- Any web site associated with this project has a "Tier 1" rating. (The Web Application Security Standard at https://getprotected.asu.edu/sites/default/files/web%20application%20security%20standard.pdf defines these ratings.)

- There are regulatory requirements that mandate Disaster Recovery and/or Business Continuity planning.
- Your project sponsor wants this considered a "Mission Critical" system for some other reason (by whatever definition is meaningful to the sponsor).

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

☐ This project has no Mission Critical components.

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

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

Additional information (optional)

If this project is "Mission Critical", please upload a copy of your plans to your google Security Review folder

and fill in the document name(s) here:

<div style="border:1px solid black; height:60px;"></div>

Logging and Alerting

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

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

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

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

Additional information (optional)

<div style="border:1px solid black; height:80px;"></div>

Software Integrity

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

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

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

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

Additional information (optional)

ASU's Software Development Life Cycle (SDLC) standard (https://getprotected.asu.edu/sites/default/files/Software_Development_Life_Cycle.pdf) calls for all software development to occur within an SDLC that includes information security controls and separation of duties to help ensure the controls are effective.

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

☐	**Unknown**	We do not know if software (including vendor software, ASU developed software, or software obtained from other sources such as libraries or frameworks) is or was developed under the control of a written SDLC.
☐	**High**	One or more software components used within this project have no SDLC.

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

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

Additional information (optional)

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

☐	**Unknown**	The status of vulnerability scanning or penetration testing is not known at this time.
☐	**High**	One or more components of new software (other than web sites) have not been vulnerability scanned or penetration tested.
☐	**Medium**	Vulnerability scanning or penetration testing has been performed, but by a member or close affiliate of the development team or vendor, such that its independence is not assured.
☐	**Low**	New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, however some issues remain unaddressed. The project team has evaluated the open issues and does not consider them a risk to ASU (explain in notes below).
☐	**Addressed**	New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, and any issues found have been addressed.
☐	**Addressed**	Vulnerability scanning or penetration testing is not required for this project because there is no new software other than web sites, and the web sites have been scanned for security vulnerabilities.

☐	**Addressed**	This project does not include any new software. Nothing new has to be installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

Additional information (optional)

Deprecated or Dangerous Technologies

Frequently an exciting new technical capability is rapidly adopted without due consideration for the security consequences. Hackers begin taking advantage of weaknesses, so some technologies carry added risk. Users can defend themselves by disallowing unwanted technologies, but then some web sites refuse to serve those users until they place themselves at risk again.

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

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

☐	**Unknown**	We do not know if the project will use any of the technologies listed in this section.
☐	**Medium**	Users are required to enable Java in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Java has become one of the top malware distribution mechanisms.)
☐	**Medium**	Users are required to permit Active-X controls. (Active-X controls give a web site more control of a user's computer, making it easier for attackers to exploit defects in the operating system, browser, or Active-X control itself. Also, dependence on Active-X locks out users of operating systems and browsers that may be more secure.)
☐	**Medium**	A password protected web site imports JavaScript code or other client-executed code from another web site that is beyond ASU's control. (This makes it possible for the other site's script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.
☐	**Medium**	A password protected web site imports JavaScript code or other client-executed code over an http (unencrypted) connection. (This makes it possible for a man-in-the-middle to inject a script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.
☐	**Low**	Users are required to enable Flash in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Flash has become a common malware distribution mechanism.)

☐	**Low**	Users are required to allow pop-up windows in their browsers. (Several popular web browsers now disable pop-ups by default because they have been abused by advertisers and malware.)
☐	**Low**	The web site only allows certain browsers, and refuses service to users of other browsers. (Such web sites frequently lock out users of operating systems and browsers that may be more secure.)
☐	**Low**	Users are required to enable or install other plug-ins or media players not listed above. (Please describe in notes below.)
☐	**Addressed**	The project uses one or more of the above technologies, but they are entirely optional. Users can still accomplish all the functions of the system even if the user shuts off the deprecated technologies.
☐	**Addressed**	The project will not use any of the technologies listed in this section.

Additional information (optional)

Other Risks

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

☐		
☐		
☐		

Additional information (optional)

Risk Score

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

Risk Rating	Unknown	High	Medium	Low	Addressed
Count of boxes checked					

Approval

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

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 <u>role</u> 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 <u>endpoint</u> in the system. Each role will be an endpoint, and each type of <u>server</u> 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 <u>connection</u> 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 <u>listening</u> for connections, usually on a predefined <u>port</u>.

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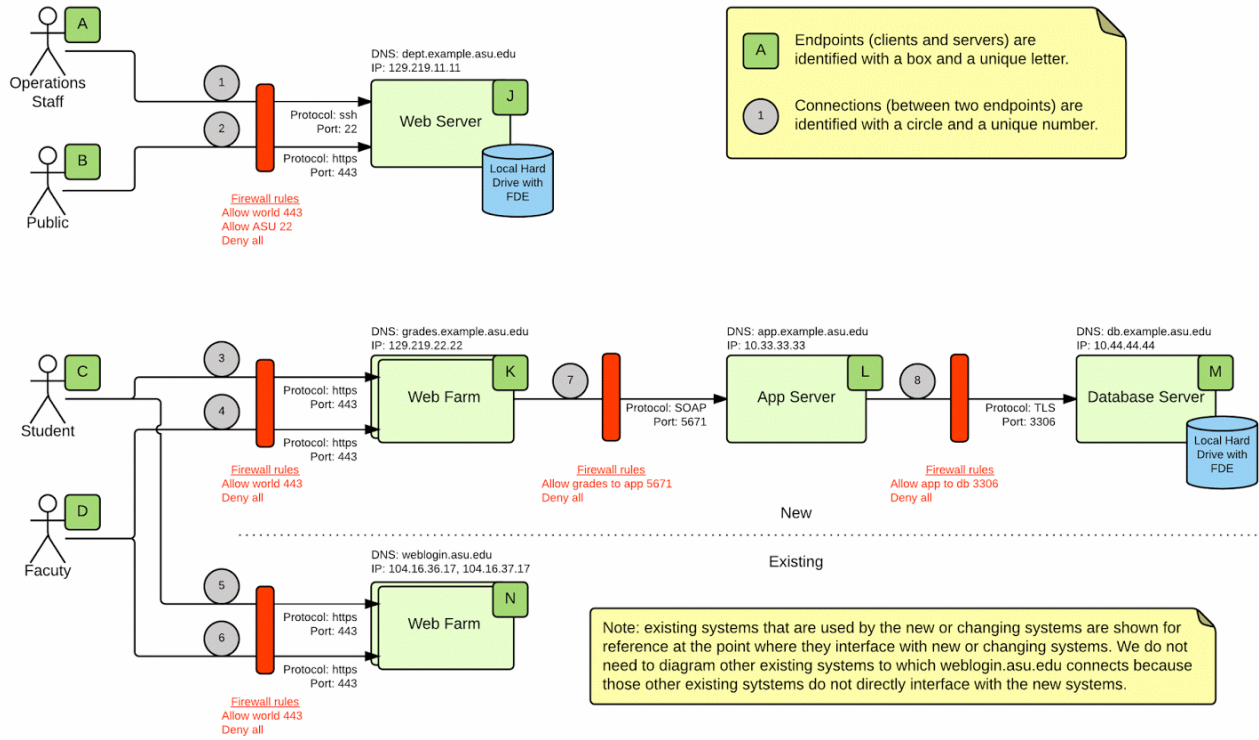
The diagram need not be colorful. Although this diagram (below) is very simple, it conveys all the requested information. Visual appeal can be beneficial, but the factual information is what really matters.
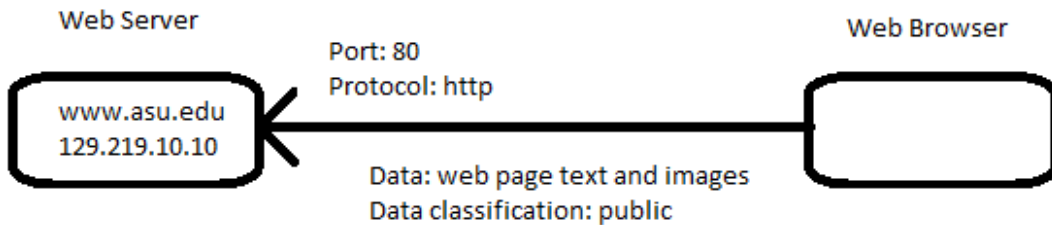
EXHIBIT A – ASU SUN CARD

Base Card PN: 2100HPC3AN		**Size:** 3.370" ± 0.005 X 2.125" ± 0.002 X 0.030 ± 0.003"	
Card Type: 2100-iCLASS 2k/2 - COMPOSITE		**Service Type:** LAMINATED ART	

Comments to the Customer:

NOTE: FRONT ARTWORK COLORS CONVERTED FROM CMYK TO PMS 123 AND PMS 208. ORIGINAL CENTER LOGO TO SMALL IN DETAIL FOR QUALITY OVI IMAGE. SUGGESTED UPDATED LOGO BELOW ENLARGED 40% WITH A .25 STROKE FOR BETTER QUALITY OVI IMAGE.

TOP **Front**   **Back** TOP

COMMON EDGE

ASU
Arizona State University

Sun Card

Emergency 911
ASU LiveSafe mobile app LiveSafe.asu.edu
ASU Help Center 1-855-278-5080

This card is governed by Arizona State University regulations. It is nontransferable. This card must be presented to secure services and authenticate privileges. A replacement fee will be charged for lost, stolen, or mutilated cards. This card remains the property of Arizona State University and must be surrendered to an authorized University Official upon request.

1/2" HICO 4000 Oe Magstripe

© HID iCLASS XX   *12345 YYYYYYYYYYY-YY SR   XT

Card surface:		**Card surface:**	
Artwork #:		**Artwork #:** BAW-02011	
Colors: PMS 123, PMS 208, OASIS OVI, BLACK		**Colors:** BLACK	

SELECT CARD TOLERANCE	· · · · = Slot Punch Indicators	12345 = Card ID Number	YYYYYYYYYYY-YY = HID Order No. - Line Item No.

Production Notes:

NOTE: MIDDLE SEAL IS OASIS OVI

EXHIBIT B – ASU GUEST CONFERENCE CARD

Base Card PN: 2100HPC3AN   **Size:** 3.370" ± 0.005 X 2.125" ± 0.002 X 0.030 ± 0.003"

Card Type: 2100-iCLASS 2k/2 COMPOSITE   **Service Type:** LAMINATED ART

Comments to the Customer:

NOTE: FONT USED IS AKZIDENZGROTESKBE-MD 7.53 PT

Front

ASU | ARIZONA STATE UNIVERSITY

guest & conference services

University Housing Affiliate

Card surface: N/A
Artwork #: AW-110675-F
Colors: MYK

Back

If found please return to:
Arizona State University – Guest & Conference Services
711 E. Lemon Street
Tempe, AZ 85281
480-965-3515
housing@asu.edu

1/2" HICO 4000 Oe Magstripe

© HID iCLASS XX   *12345 YYYYYYYYYYY-YY   XT
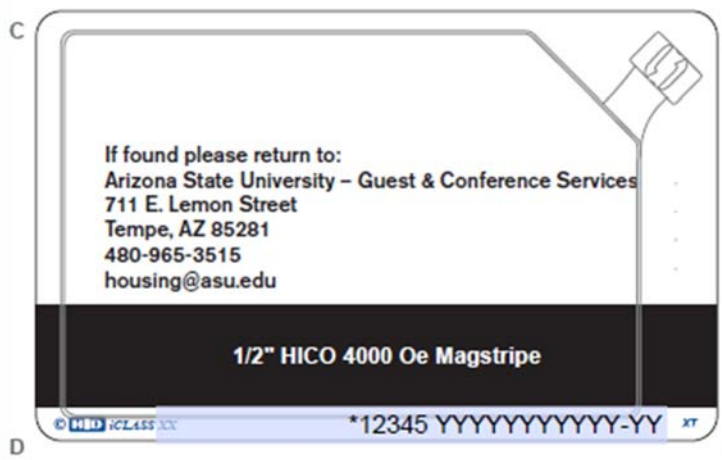
Card surface: N/A
Artwork #: AW-110675-B
Colors: BLACK

| Tolerance of Image Location = +/- .020 | - - - - = Slot Punch Indicators | 12345 = Card ID Number | YYYYYYYYYYY-YY = HID Order No. - Line Item No. |

EXHIBIT C – ASU PROHIBIT SUN CARD

*Non iCLASS

PROOF

07-20-18
QUANTITY = 3000 (EXACT)
SIZE = 30 MIL CR80 PVC (2.125" X 3.375")

OVERLAMINATED
PRINTED CMYK ON FRONT TO MATCH PREV ORDER
PRINTED BLACK ON BACK
½"HE (2750 OE) MAGNETIC STRIPE ON BACK
SHRINKWRAPPED IN 100'S

(+/- .063" TOLERANCE ALLOWABLE FOR MOVEMENT
DURING PRODUCTION)

SLOT = NONE
BARCODE = NONE
CONSECUTIVE START NUMBER = NONE
ENCODING = NONE

HERE IS THE PROOF FOR YOUR ORDER. PLEASE REVIEW CAREFULLY. IF YOU
HAVE NOT PROVIDED LINE ART FOR YOUR COPY, TEXT AND DESIGN ELEMENTS MAY
HAVE BEEN TRACED AND/OR RE-TYPED FOR THE BEST PRINT QUALITY. PLEASE
PROOFREAD ALL TEXT VERY CAREFULLY FOR ANY TYPOGRAPHICAL ERRORS. WE
WILL NOT BE RESPONSIBLE FOR TYPOGRAPHICAL OR DESIGN ERRORS AFTER
APPROVAL OF THIS FORM. THIS FORM MUST BE SIGNED AND FAXED BACK BEFORE
JOB CAN PROCEED.

**A SIGNED PROOF ESTABLISHES FULL
RESPONSIBILITY BY THE SIGNER. THANK YOU.**

ART APPROVED

TOP FRONT

ASU
Arizona State University

Sun Card

TOP BACK

Emergency 911
ASU LiveSafe mobile app LiveSafe.asu.edu
ASU Help Center 1-855-278-5080

This card is governed by Arizona State University regulations, It is nontransferable. This card
must be presented to secure services and authenticate privileges. A replacement fee will be
charged for lost, stolen, or mutilated cards. This card remains the property of Arizona State
University and must be surrendered to an authorized University Official upon request.

½" HE (2750 OE) MAGNETIC STRIPE

EXHIBIT D – POS EQUIPMENT

Campus	Building	Title	Workstation Type	Cash Drawer's	Receipt Printer	IP Printer	KDS
West	914 - Verde Dining Pavilion	Verde Dining Hall	WS 5s	2	1		
West	900 - Fletcher Library	Starbucks	WS 5s	2	1		
West	900 - Fletcher Library	Starbucks	WS 5s	2	1		
West	914 - Verde Dining Pavilion	Verde Dining Hall	WS 5s	2	1		
West	915 - Verde Dining Pavilion	Verde Dining Hall	WS 5s	2	1		
West	914 - Verde Dining Pavilion	Verde Dining Hall	WS 5s	2	1		
West	903 - University Center Building	Cafe West	WS 5s	2	1		
West	904 - University Center Building	Cafe West	WS 5s	2	1		
West	903 - University Center Building	Cafe West	WS 5s	2	1		
West	Fletcher Library	Starbucks	WS 5s	2	1		
West	Fletcher Library	Starbucks	WS 5s	2	1		
West	914 - Verde Dining Pavilion	Jamba Juice	WS 5s	2	1		
West		West Market	WS 5s	2	1		
West	912 - Welcome Center	Sun Card	WS 5s	1			
Tempe	035 - Memorial Union	AFC Sushi	WS 5s	2	1		
Tempe	173G - Barrett College Willow Hall	Barrett Dining Hall	WS 5s	2	1		
Tempe	173G - Barrett College Willow Hall	Barrett Dining Hall	WS 5s	2	1		
Tempe	173G - Barrett College Willow Hall	Barrett Dining Hall	WS 5s	2	1		
Tempe	1048 - Biodesign Institute B	Charlies	WS 5s	2	1		
Tempe	010 - Hayden Library	Charlies	WS 5s	2	1		
Tempe		Charlies	WS 5s	2	1		
Tempe	035 - Memorial Union	Chick Fil A	WS 5s	2	1		1
Tempe	035 - Memorial Union	Chick Fil A	WS 5s	2	1		
Tempe	035 - Memorial Union	Chick Fil A	WS 5s	2	1		
Tempe	035 - Memorial Union	Chick Fil A	WS 5s	2	1		
Tempe	035 - Memorial Union	Chick Fil A	WS 5s	2	1		
Tempe	050 - Wilson Hall	Daves Dogs	WS 5s	1	1	1	
Tempe	050 - Wilson Hall	Daves Dogs	WS 5s	1	1	1	
Tempe	035 - Memorial Union	Devils' Greens	WS 5s	2	1		
Tempe	035 - Memorial Union	Devils' Greens	WS 5s	2	1		
Tempe	035 - Memorial Union	Engrained	WS 5s	2	1	1	
Tempe	035 - Memorial Union	Engrained	WS 5s	2	1	1	
Tempe	035 - Memorial Union	Engrained	WS 5s	2	1	1	
Tempe		Fresh	WS 5s	2	1		
Tempe		Freshii	WS 5s	1	1	1	
Tempe	163A - Hassayampa Mesquite Hall	Hassayampa Dining Hall	WS 5s	2	1		
Tempe	163A - Hassayampa Mesquite Hall	Hassayampa Dining Hall	WS 5s	2	1		
Tempe	163B - Hassayampa Verbena Hall	Hassayampa P.O.D	WS 5s	2	1		
Tempe	035 - Memorial Union	Jamba Juice	WS 5s	2	1		
Tempe	035 - Memorial Union	Jamba Juice	WS 5s	2	1		
Tempe	061 - Manzanita Hall	Manzy Square	WS 5s	2	1		
Tempe	061 - Manzanita Hall	Manzy Square	WS 5s	2	1		
Tempe	035 - Memorial Union	Outta' Here	WS 5s	2	1		
Tempe	051F - Palo Verde East	Palo Verde Market	WS 5s	2	1		
Tempe	035 - Memorial Union	PEI WEI	WS 5s	2	1	1	
Tempe	035 - Memorial Union	PEI WEI	WS 5s	2	1	1	
Tempe	035 - Memorial Union	PEI WEI	WS 5s	2	1	1	
Tempe	035 - Memorial Union	Pitchforks Residential Restaurant	WS 5s	2	1		
Tempe	035 - Memorial Union	Pitchforks Residential Restaurant	WS 5s	2	1		
Tempe	035 - Memorial Union	QDoba	WS 5s	2	1		
Tempe	035 - Memorial Union	QDoba	WS 5s	2	1		
Tempe	138 - Sonora Annex	Sonora Market	WS 5s	2	1		
Tempe	Memorial Union	Starbucks	WS 5s	2	1		
Tempe	Memorial Union	Starbucks	WS 5s	2	1		
Tempe	051F - Palo Verde East	Starbucks	WS 5s	2	1		
Tempe	051F - Palo Verde East	Starbucks	WS 5s	2	1		
Tempe	035 - Memorial Union	Subway	WS 5s	2	1		
Tempe	035 - Memorial Union	Subway	WS 5s	2	1		
Tempe	HASS	Subway	WS 5s	2	1		
Tempe	HASS	Subway	WS 5s	2	1		
Polytechnic		Subway	WS 5s	2	1		
Poly		Cafe Poly	WS 5s	2	1		
Poly		Citrus	WS 5s	2	1		
Poly		Starbucks	WS 5s	2	1		
Poly		Party Dog	WS 5s	2	1		
Poly		Citrus	WS 5s	2	1		
Downtown	306A - Taylor Place South Tower	Taylor Place Market	WS 5s	2	1		

Downtown	301 - University Center	City Cafe	WS 5a	2	1		
Tempe		Tooker House	WS 5a	2	1		
Tempe		Tooker House	WS 5a	2	1		
Downtown	306A - Taylor Place South Tower	Taylor Place Residential Resturaunt	WS 5a	2	1		
Downtown	306A - Taylor Place South Tower	Taylor Place Residential Resturaunt	WS 5a	2	1		
Downtown	301 - University Center	City Cafe	WS 5a	2	1		
Downtown	301 - University Center	City Cafe	WS 5a	2	1		
Downtown	306A - Taylor Place South Tower	Starbucks	WS 5a	2	1		
Downtown	306A - Taylor Place South Tower	Starbucks	WS 5a	2	1		
Downtown		POD	WS 5a	2	1		
Downtown	Taylor - Chick Fil A	Chick Fil A	WS 5a	2	1		1
Downtown	Taylor - Chick Fil A	Chick Fil A	WS 5a	2	1		
Downtown	Taylor - Chick Fil A	Chick Fil A	WS 5a	2	1		
Downtown	Taylor - Chick Fil A	Chick Fil A	WS 5a	2	1		
Downtown	Taylor - Chick Fil A	Chick Fil A	WS 5a	2	1		
Downtown		The Market	WS 5a	2	1		
Downtown	LAW	Engrained	WS 5a	2	1	1	
Downtown	LAW	Engrained	WS 5a	2	1	1	
Downtown	LAW	Engrained	WS 5a	2	1	1	
Tempe		Tooker House	WS 5a	2	1		
Tempe		Chick-in	WS 5a	2	1		
Tempe	Armstrong	EBB_ARMSTRONG	WS 5a	2	1	1	
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 142	Verifone				
Tempe	ASU Stadium	South Concessions 140	Verifone				
Tempe		Hassy Market	Micros Compact 310				
		Tooker Market	Micros Compact 310				
		MU Market	Micros Compact 310				
		MU Market	Micros Compact 310				
		MU Market	Micros Compact 310				
Downtown		Taylor Place Market	Micros Compact 310				
Poly		Poly Market	Micros Compact 310				
West		West Market	Micros Compact 310				
Poly		Party Dogs	Micros Compact 310				
Tempe		Special Events	Micros Compact 310				
				174	88	14	2