



## **Procurement and Contracting Services**

### **Request for Proposals for an RFID-Based Library Security Gate Solution**

#### **ADDENDUM #1**

**Please mark all proposal submission**

**Envelopes with the following information**

**Sealed RFP #L232204**

**Due on July 6, 2022, no later than 2:00 PM/MST**

The following questions have been received by the technical question due date of June 23, 2022, by 12:00 PM/MST.

1. How many RFID tags are required for books?

a. UAL has approximately 4 million physical items in our collection.

2. Does the University require AV tags?

a. Yes.

3. Will the University tag all items or just a portion of its collections?

a. RFID tags will be added to a portion of the collection to start. We will likely expand the RFID tagging over time.

4. Your deadline for installation is coming up very quickly. When does the University plan to award? When does the University plan to provide the PO?

a. The RFP closes on July 6<sup>th</sup>, and we hope to review all proposals and select a vendor by the following week. If there are any further clarifications, we will need to address those first before moving forward with the award. We will then begin negotiations on a contract with intent to sign about 10 days after notification of award. The PO will be issued after the RFP is awarded and once a contract is fully executed. Please provide us with your estimated timeline from contract signing for the installation and operational use of the equipment.

5. Please confirm that the University wants physical installation required on or before August 1, 2022. Does this include the gates and staff stations?

a. The physical installation on August 1<sup>st</sup> does include the gates. The installation of staff stations could occur later. While August 1<sup>st</sup> is our initial estimated installation date, we understand this date is quickly approaching. Please provide us with a timeline for how long after a signed contract and PO is issued that the physical installation of the gates and staff stations would take to be completed.

6. Can you confirm that the University wants the gates installed, but not operational, on or before August 1?

a. While August 1<sup>st</sup> is our initial estimated installation date, we understand this date is quickly approaching. Please provide us with a timeline for how long after a signed contract and PO is issued that the physical installation of the gates and staff stations would take to be completed. If this date does not include the gates being operational, just installed, please also provide us with the timeline for when they would be operational.

7. Can you confirm the University has power and data at each RFID gate location that is ready for gate set-up and configuration prior to August 1?
  - a. All RFID gate locations will have access to specified power and data once a vendor has been selected and the specific needs of the adopted solution are known.
8. What is the University's tax rate for the requested solutions?
  - a. Total tax rate: 8.20%
    - i. Arizona Tax Rate – Pima County – Use Tax Purchases: 5.60%
    - ii. City of Tucson – Use Tax Purchases: 2.60%
9. In regard to Section 5.6.2, are you only requesting software maintenance and support, or do you want us to also provide a quote for on-site hardware maintenance and parts?
  - a. We are requesting information on all options for both ongoing software and hardware maintenance costs.
10. Regarding Section 5.2.1.2, can you please clarify how you want the gates to integrate with your current self-check solution?
  - a. We would like to understand if your solution can be integrated with current Self Check solution (Envisionware X11 countertop and Kiosk models) or if we will need to purchase a different self-check solution. Integration includes the ability of the self-check to successfully disarm/deactivate the RFID tag upon successful checkout of an item which will allow patrons to exit through the gates without triggering an alert.
11. Regarding Section 5.2.1.3.2, can the University share with us what type of non-University affiliates are being referred to and how the cards would be used in this section?
  - a. In addition to the students, staff and faculty of the University of Arizona, the University Libraries also allow members of the wider Arizona community (state residents, students and faculty from other state universities and colleges etc.) to acquire or purchase a borrower's card that allows them circulation privileges from our collections. Currently the cards issued use a magnetic strip for data storage which includes a pre-programmed 16-digit barcode.
12. Regarding Section 5.2.2.4, can you please clarify why self-check stations are listed here?
  - a. Most of our print collections are circulated through one of five deployed self-check stations. We anticipate that this pattern will continue and see the self-check stations along with staff workstations and security gates as components of a unified circulation workflow. We would like to understand what (if any) data is captured by a station as part of the lending/checkout process/workflow. Especially if the data captured pertains to patron accounts or other personally identifiable information.

13.Regarding Section 5.2.2.5.1, can you please clarify why self-check stations are listed here?

- a. Most of our print collections are circulated through one of five deployed self-check stations. We anticipate that this pattern will continue and see the self-check stations along with staff workstations and security gates as components of a unified circulation workflow. We would like to understand any requirements that might pertain to local administrative rights for any hardware as well as the need for any type of local client software.

14.Regarding Section 5.2.2.6.2, are you requiring a central management and reporting application for to be capable of managing all your current self-checks and gates? If so, only one vendor can provide this.

- a. No, we are not requiring a central management and reporting application. We would like to understand any integrated reporting or analytics tools included with your solution. The degree to which outputs from these tools can be accessed and customized locally and the degree to which data from these reporting or analytics tools can be integrated with other third-party analysis and visualization tools like Tableau, MS Power BI, Google Data Studio etc.

15.Regarding Sections 5.4.2.2, 5.4.2.3, and 5.4.2.4, can you please clarify how the loaning and returning of items from a self-check is part of the scope of work for the acquisition of gates and staff workstations?

- a. Most of our print collections are circulated through one of five deployed self-check stations. We anticipate that this pattern will continue and see the self-check stations along with staff workstations and security gates as components of a unified circulation workflow. Under our current model, our self-check stations also give patrons the ability to check-in returned items without direct staff mediation. We would like to understand how your proposed solution could accommodate this workflow.

16.Regarding Section 4.53.2.4, how does the University handle penetration testing? Does the University provide a tool to the vendor to perform testing?

- a. No, vendor must source a tool at their own expense to perform the testing outlined in section 4.53.2.4.

17.Regarding Section 4.53.1.1, what are the written confidentiality obligations?

- a. These may vary in form. Vendor can detail how they control their written confidentiality obligations on their end by employees, auditors, and hired contractors. Please detail your process of this section in your submission. In addition, the agreement with awarded vendor will include confidentiality clauses therein which can act in part as written confidentiality obligations. When contract negotiating with awarded vendor, specific details can be finalized as needed.

18. Regarding Section 4.53.2.4, the requested systems do not lend themselves to vulnerability scanning as the vendor does not control the hardware on which the software packages are installed. Why is the University requesting vulnerability and penetration testing and annual audits for the requested solutions?

- a. If applicable, vendor must detail how their hardware and software installation system would not be vulnerable to items as detailed in section 4.53.2.4. Along with that detail, all systems will still be required to meet the obligations detailed in this section as to the testing and audit requirements to ensure hardware and software systems are still performing at peak levels and are not left vulnerable.

**End of addendum, all else remains the same.**