Procurement and Contracting Services

Request for Proposals:
Contact Center as a Service (CCaaS)

ADDENDUM #4
PCI/DSS and PBAP Compliance Language

Please mark all proposal submission
Files with the following information

Sealed RFP # L312501
Due on April 30, 2025, no later than 1:00 PM, MST

RFP #L312501 - Addendum 4

Context:
The original RFP posting includes PCI/DSS compliance as required in Limiting criteria of section 3.9.8. However, section 4.51 of the Agreement Terms is incorrectly labeled as “Not Applicable”.

Change to RFP Section: 4.51

- **PCI DSS and PABP Compliance.** Contractor acknowledges, warrants and will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data and/or sensitive authentication data and/or can affect security of those entities that store, process, or transmit cardholder data (e.g. Managed Services).

  Furthermore, Contractor must certify at time of contract/agreement to be in compliance and continue to meet all applicable requirements by providing validation either by appearing on the VISA Global Registry of Service Providers (CISP), Payment Card Industry Security Standards Council Validated Payment Applications list (if applicable), or provide a completed and signed Attestation of Compliance (AOC) signed by a PCI approved Quality Security Assessor (QSA). Any change in Contractor’s certification requires prompt (within thirty (30) days) written notification to the University of Arizona.

  Furthermore, Contractor agrees to provide to the University of Arizona upon request, any supporting compliance documentation such as but not limited to Approved Scan Vendor (ASV) Attestation of Compliance (AOC), external scan results, penetration testing results, and/or a completed Service Provider Self-Assessment Questionnaire (SAQ) D (if not completing a third-party assessment).

  Contractor agrees to indemnify the University for any breach of its cardholder data attributed to the application, system, or Contractor controlled interface to CHD or service provided by the Contractor. Contractor agrees to notify the University authorized representative within 24 hours in the event of unauthorized release of cardholder data.

  Contractor must provide written documentation, which outlines the specific PCI DSS compliance responsibilities of both the Contractor and the University.

Summary of Change:
PCI/DSS compliance language has been restored to the appropriate RFP section 4.51.

[End of Addendum. All else remains the same.]