

KMS RFP VENDOR QUESTIONS AND ANSWERS

1. *What is the total size of data in terabytes?*

Answer: LACERA houses most of its knowledge assets in SharePoint and lacera.gov. Currently, the SharePoint content is 15.5 TB and the content on our website is 10.9 GB. However, the size of the data is subject to change and will likely increase.

2. *Is a DR environment a requirement of this program to ensure uptime availability in the event of catastrophic failure?*

Answer: Yes.

3. *Could you clarify whether the term “cloud-first” reflects a preference for self-hosted cloud deployment or a fully managed (SaaS) model? Additionally, is there a preferred cloud provider (e.g., Azure, AWS, or another platform)? (In Reference Technical Requirement: Must adhere to a cloud-first strategy, prioritizing deployment in a secure and scalable cloud environment unless specific business, regulatory, or technical constraints justify an native approach.*

Answer: The term “cloud-first” reflects a preference for deployment in a secure and scalable cloud environment rather than an on-premise solution. LACERA does not seek an on-premise approach for this engagement. There is no stated preference for a specific cloud provider; the focus is on ensuring reliability, data protection, and seamless integration with existing systems. Both fully managed (SaaS) solutions and other secure cloud-hosted models are acceptable, provided they align with these priorities.

4. *Can LACERA indicate where this policy can be found for review and agreement? (Referencing 2.3 Functional Requirements – 1.6 Vulnerability Management, “The Vendor must adhere to LACERA’s Vulnerability Management Policy.”)*

Answer: LACERA maintains a formal Vulnerability Management Policy to ensure consistent security practices across all systems and vendors. A copy of this policy can be shared with a vendor only after a Non-Disclosure Agreement (NDA) has been executed between both parties.

5. ***For software licensing, should respondents propose pricing for a one-year term, a multi-year term (example: three years), or both?***

Answer: Please provide both: a one-year and three-year terms.

6. ***Can LACERA confirm that an enterprise taxonomy is already in place, and whether it includes terminology that is member-friendly (either as preferred labels or synonyms)?***

Answer: There is an enterprise taxonomy that represents a third of the LACERA divisions, which are member-facing. The current emphasis is on staff use. However, the intention is that the taxonomy will be extended as appropriate to public-facing knowledge assets and other LACERA divisions.

7. ***To support planning assumptions, could LACERA outline which AI-enabled capabilities - besides chatbots - are expected to connect with or consume data from the KMS?***

Answer: LACERA would like AI capabilities such as, but not limited to, tagging and re-tagging content, taxonomy maintenance, search, summarization, translation, and question answering. In addition, LACERA would also like AI to interact with other applications such as Genysys to retrieve information. In the future AI may perform analysis of written correspondence, member scenarios, and business challenges and access the KMS to use the knowledge therein to provide recommendations.

8. ***Aside from SharePoint, are there any other knowledge repositories or content systems expected to be integrated with the KMS?***

Answer: Currently, the majority of LACERA's knowledge assets are stored in SharePoint and lacera.gov, but should be extensible to other applications, e.g. ServiceNow, Confluence, etc.

9. ***Has LACERA already established the asset-sensitivity categories, particularly those governing access for an externally facing member chatbot? And can LACERA confirm that defining these categories is out of scope for this engagement?***

Answer: LACERA currently has categories such as, "Strictly confidential" (includes PII), "Confidential" (everything else unless approved for public), and "Public" (on lacera.gov). But sensitivity labels have not been established or systematically applied to all assets in SharePoint libraries. LACERA will define the asset-sensitivity categories.

- 10. *Provide your response to the enclosed Questionnaire (Exhibit C). Excluding the requested Exhibits and Attachments, your response must not exceed 60 pages. "Please confirm whether the 60-page limit applies solely to the main proposal narrative or also includes exhibits, attachments, and supplemental materials.***

Answer: Exhibits A, B, D, E, G, H, and resumes added as vendor exhibits and attachments are excluded from the 60-page limit. Answers to Exhibit C Questionnaire are subject to the 60-page limit.

- 11. *Beyond the stated functional requirements, should respondents consider any additional requirements relevant to this section?***

Answer: Please refer to Section 2.2 of the RFP for the functional requirements.

- 12. *Can you confirm that LACERA currently owns the O365 and SharePoint products, so the bidder should not include their costs in the proposal?***

Answer: Yes, LACERA owns O365 and SharePoint.

- 13. *Can you comment on the maturity of the current SharePoint implementation at LACERA and whether it already meets certain requirements listed? This will help inform the level of effort needed to mature your O365/SharePoint to meet stated requirements.***

Answer: LACERA's SharePoint implementation needs maturing for knowledge management purposes, e.g., TermStore is just beginning to be implemented, there is no Purview framework yet, etc.

- 14. *What cloud providers does LACERA currently use for its infrastructure? (Azure, AWS, GCP, etc.) Is there a preference for this opportunity?***

Answer: LACERA leverages industry-standard cloud technologies to support its infrastructure needs, focusing on security, scalability, and compliance. For this opportunity, there is no stated preference for a particular provider. The primary consideration is ensuring reliability, data protection, and seamless integration with existing systems.

15. ***"Exhibit D Agreement for Services Item 17 SOC 2 states that an annual report is required for the Vendor and all subcontractors handling confidential information. Our SaaS solution is built on AWS storage and services and does not require us to have access to the actual data stored within the application to install, configure, and support it. In previous engagements, with a SOC 2 requirement, providing the AWS SOC2 report satisfied the requirement.***

Would an AWS SOC2 report suffice in meeting this Annual SOC2 Report requirement?

Answer: LACERA must ensure and monitor the security of the selected vendor's systems. The scope of the required report will be a subject for discussion with the selected vendor in finalizing the contract based on the vendor's approach and technology. However, generally, an AWS SOC2 production every year and a certification from the vendor that they have not accessed the data would suffice. Further, any loss of data or breach of data will need to be reported to LACERA within 24 hours.

16. ***"In Attachment E IT Security controls it states:***

IF RESPONDENTS HAVE NOT COMPLETED ANY OF THE ABOVE COMPLIANCE REPORTS, THEY MUST COMPLETE AND SIGN THE VENDOR DATA SECURITY QUESTIONNAIRE DOCUMENT IN ORDER TO ASSESS THEIR SECURITY POSTURE AND SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS, INFORMATION FUNCTIONS, AND PROCESSES."

Does this mean filling out the security questionnaire fulfills the requirement for a SOC Report, or may a SOC Report still be required for the Vendor and all Subcontractors? "

Answer: A SOC report will still be required.