CoSD Procurement Guidelines for Artificial Intelligence Products and Services

These procurement guidelines shall apply in situations where the County is acquiring a software application that utilizes or contains artificial intelligence to ensure County data is protected and County AI policies are adhered to. All product vendors shall be asked to submit written responses to the following questions and statements. Vendor responses and statements may be placed in the licensing agreement with the vendor to ensure County interests and data are protected and not been mis-characterized by the product vendor.

1. Characterize the artificial intelligence (AI) product the vendor product is utilizing:
    a. Please describe the pre-trained (possibly domain specific) Models.
        i. Explain the application programming interface (API) used for input and harvesting output.
    b. Please describe the Fine-Tuned Models used.
        i. Explain how the initially pre-trained AI vendor model; augmented with product vendor training data.
        ii. Explain the API used for input and harvesting output.
    c. Please describe the Self-Trained Models.
        i. Explain the exclusively trained on product vendor data.
        ii. Explain the API used for input and harvesting output.
2. If Fine-Tuned or Self-Trained Models are being utilized by the product vendor:
    a. Please describe the product vendor's training data curation and archiving plan.
    b. Please describe active countermeasures taken to protect against prompt injection attacks and training data poisoning (see CoSD AI Security Checklist: Items 2 and 4).
3. Generally, County data cannot be integrated into the AI vendor's product model. If County input data will be integrated into the AI vendor's product model, a County Technology Office waiver must be obtained. Will County data be integrated into the AI vendor's product model?
4. Even if the AI vendor will not integrate County data into its generative AI model; the AI vendor must also agree not to sell or share County input or generated output data to other parties. Further, the product vendor itself and/or the AI vendor cannot use the County data for any other purpose within their companies. Deviation from these guidelines requires a waiver from the County Technology Office.
5. The AI vendor should be using both Data Loss Prevention methods and output filters to protect accidental input or output of PII/PHI/HIPAA/PCI and to guard against harmful, discriminatory or otherwise offensive output. If not, a County Technology Office waiver must be obtained.

6. The AI vendor should be using well-defined APIs and adhere to pentation testing standards to ensure compatibility with other systems.

7. Please provide vendor exit strategies or portability capabilities to ensure a smooth transition to another product if the situation should arise.

8. Please complete the attached CoSD AI Security Checklist to address the AI vendor's mitigations against generative AI bias, threats and the trustworthiness of the AI vendor's AI solution.

9. If the County architect deems active risk management necessary for the AI vendor's generative AI solution being used in the product vendor solution because of answers obtained from the CoSD AI Security Checklist, a County Technology Office waiver must be obtained.

10. County and vendor relationships need to include a set cadence or annual review of feature roadmaps and communications on changes that improve the County, introduce risk or may or may not include training needs for County users. This will strengthen the benefits of AI and vendor provided solutions.