# **A picture containing text, clipart Description automatically generatedKCMO PRELIMINARY VENDOR SECURITY QUESTIONNAIRE**

FORM 2- CONFIDENTIAL and PROPRIETARY

This vendor or 3rd party-vendor cybersecurity questionnaire is required to be completed by all potential vendors proposing or already doing business with the City of Kansas City, Missouri (KCMO) or with any KCMO affiliated agency or department.

Additional information may be requested depending on the answers or lack of answers that are provided. (Please attach all related information and documentation including contact information).

This information has been deemed non-discoverable under the MO Sunshine Law. The City will not be releasing this form under the MO Sunshine Law.

(Vendor/Supplier/Service Provider Name and description of services to be provided to the City of KCMO must be entered in this paragraph)

**Vendor Questions:** Each yes or no question must be checked, All N/A answers must be explained as these questions are related to your general and specific cybersecurity business practices. Please provide requested details under each question or append to the end of this document with reference to the specific question being answered

Yes  No - Does your company have a written control plan that contains the administrative, technical, and physical safeguards you use to collect, process, protect, store, transmit, dispose, or otherwise handle KCMO data (e.g., Information Security Plan)? If yes please attach, if no please explain why not.

Yes  No - Does your system or application which will be storing our client data provide access control mechanisms (e.g., unique user IDs, passwords standards, role-based access)? If yes please explain them and if no, please explain why not.

Yes  No - Does your system or application provide multi-tenant controls for physical and/or logical separation of users and data within the service? If yes, please provide policy/procedures. If no, please explain why not.

Yes  No - Does your company utilize encryption and masking techniques/methods for data at rest, in transit, and when displayed? If yes please explain i.e.use of data serialization and masking for privacy. If no, please explain why not.

Yes  No – Does your company have a written business continuity/disaster recovery plan, which is tested on a periodic basis? If yes KCMO may request a copy of the plan at some point during this agreement period, If no please explain how your business will operate in emergency situations such as the National Covid pandemic.

Yes  No - Does your company have a dedicated/contracted cybersecurity team to ensure adequate steps are taken to guard against unauthorized access to client data? If yes please list the group/contractor and what cybersecurity support services, they provide. If no please explain how your company manages this risk.

Yes  No - Does your company maintain up-to-date versions of anti-virus software, anti-malware, antispyware, and operating systems security patches? If yes how is this managed, if no please explain why not.

Yes  No - Will your company actively monitor and manage your IT security environment to prevent security incidents or breaches? If yes what tools and/or services do or will you use to perform this function and if no, please why not.

Yes  No - Does your company perform application security testing? If yes please describe and provide samples along with methodology. If no, please explain why not.

Yes  No - Does your company have a written plan to promptly identify, report, and respond to breaches of security related to KCMO data (e.g., incident response plan)? If yes, please provide and if no please explain why not.

Yes  No - Will any third-party vendors (e.g., subcontractor, managed shared hosting) be used by your company and be restricted from having access to the system or application data of KCMO? If yes, please explain how you will manage this and if no please confirm that you do not allow any 3rd party vendors access to any of your data or systems either related or not related to this agreement with KCMO.

Yes  No – Will your company provide assurance (in the form of a written report) for you and your third-party vendor's security and controls while any KCMO data is being collected, processed, and retained? If yes, please provide your most current report and if no please confirm that you do not allow any 3rd party vendors access to any of your data or systems either related or not related to this agreement with KCMO.

Yes  No Can you provide the results of your last security audit you have for your company and any relevant third-party service provider your company contracts. If no please explain why not.

Yes  No Can you provide the specific services that are included in the KCMO monthly service fee and what services will be an additional fee?

What is or will be the length of this contract? What is or will be the Service Level Agreement (SLA) with KCMO and how often is KCMO able to change or modify this SLA?

# ADDITIONAL INFORMATION

1. KCMO reserves the right to perform an audit at any time during the term of any agreement between KCMO and a vendor to verify their compliance with the answers provided.
2. KCMO may require additional information based on the answers or lack of answered provided.
3. Vendors should provide copies of requested documentation including any certifications, prior assessments, or test results.