连云港市政府采购合同

（合同编号：***）

甲方：（买方）连云港市财政局

乙方：（卖方）江苏移动信息系统集成有限公司

甲、乙双方根据 2025 年 11 月 06 日 市财政局数据安全管控建设及日常驻场运维保障服务 项目（项目编号：JSZC-320700-XHZX-C2025-0035）竞争性磋商采购的结果，签订本合同。

一、合同内容

1.1 服务内容：数据安全管控体系合规建设——数据分类分级：

对市财政局开展数据分类分级合规工作，通过科学有效的分类分级体系，使市财政局可以更好地监控和管理敏感数据，确保其安全、合法地使用和共享。

数据安全管控体系接口安全——API 风险监测系统：

在前期的数据安全检查工作中，发现了部分数据安全风险。这些问题主要集中在部分业务系统的接口上。开展常态化的应用接口安全监测能力建设建立完善的安全防护体系，定期进行安全检查和评估，及时发现并处理安全隐患。提高应用接口性能，确保其在高负载下稳定运行。

此外，确保财政系统账号安全，防止非法使用，需要严格监控账号使用情况，并在发现异常时立即处理。

数据安全管控体系数据库安全——数据库防火墙系统：

在前期检查过程中，发现数据库安全协议漏洞绕过风险。需建立数据库安全防护能力，从访问控制、风险监测、人员管控等维度全面安全加固，保障数据库稳定运行，更快地处理和响应请求。

数据安全管控体系文档安全——数据防泄露系统：

在前期检查过程中，发现大量文件承载敏感数据，虽未造成外发风险，但应加强敏感文件的安全防护，有能力控制敏感文件违规外发。因此，本次项目需加强敏感文件的防泄漏措施，采用先进的技术和方法，以提高整体的信息安全水平。

市财政局信息化日常驻场运维保障服务内容：

局内外局域网（各楼层弱电间网络设备维护）的监控、调试维护；2、局内外网电脑的定期维护、系统清理及其他应用软件的维护；3、局网络运维管理系统平台（飞思网巡平台、网络管控和准入平台等）的查看、监控及故障处理；4、协助信局息中心做好其他工作。

1.2 服务要求： 数据分类分级服务：本次数据分类分级服务，完成不低于 5 万个字段的数据分类分级，提交《分类分级策略清单》、《数据分类分级清单》。形成敏感数据分类分级清单。沉淀符合本单位的数据分类分级策略，为数据分类分级工作提供规范化流程和标准化技术规范支撑，提升本单位数据安全合规以及管理水平。提供分类分级专家服务，快速实现自动化的数据分类分级，提高分类分级效率。

API 风险监测系统

类别	指标项	详细参数
性能要求	采集范围	镜像流量不低于 1G，http/https 日志采集不低于 500M。
数据接入	流量接入	流量接入方式：系统支持旁路镜像、Agent 接入、第三方日志的方式接入流量。可同时支持旁路镜像、Agent、第三方日志多种方式组合接入流量，并区分流量来源。
数据识别	敏感数据识别	敏感数据识别：支持个人敏感数据识别，至少包含 100+个人敏感数据标签。可自定义新增业务敏感数据标签和类型。对数据识别位置进行配置，包含 Request 和 Response 内容提取。对识别策略进行自定义配置，包含正则、词组、自定义算法等进行组合配置识别。
	API 拆分	▲支持 API 拆分功能，需支持根据请求方法、请求 Header 中的参数、Get 请求中的参数、Post 请求中的参数对 API 进行拆分。（投标人提供功能截图并加盖供应商公章）

API 资产分析	API 资产识别	支持通过流量还原 API 接口，输出 API 接口清单、应用清单等。支持在一个页面展示 API 敏感等级、API 风险等级、API 累计访问次数、API 流量来源、API 单次返回最大数据量、API 审计状态、请求方法、弱点数量、风险数量、API 状态、API 标签、API 格式、访问域、部署域、终端类型、请求类型、返回类型、请求数据标签、返回数据标签、资产类型、首次发现时间、最近活跃时间等。可基于筛选出来的 API 资产清单，导出为列表格式、burp 格式，导出的字段可自定义选择。
	API 归类	▲支持根据 API 接口的使用场景、调取访问方式、访问域、部署域等信息自动对接口进行自动梳理和归类，内置分类至少包括登录 API、文件上传 API、文件下载 API、数据采集 API、数据使用 API。（投标人提供功能截图并加盖供应商公章）
	API 画像	支持展示 API 详细信息。API 基本信息应包含 API 名称、应用、API 格式、API 标签、流量来源、资产类型、请求方法、请求类型、终端类型、访问域、部署域、返回类型等。数据访问信息应包含累计访问次数、API 敏感等级、API 风险等级、弱点数量、风险数量、弱点事件、风险事件、请求数据标签、返回数据标签、单次返回最大数据量等。其他关联信息应包含审计状态、确认状态、API 状态、首次发现时间、最近活跃时间等。可自定义时间段，查看 API 接口的访问次数趋势。
弱点识别能力	弱点识别	▲支持弱点识别，可按照 Owasp API Top10 进行分类识别。（投标人提供功能截图并加盖供应商公章）

	弱点功能	API 弱点功能要求，内置弱点识别至少包括参数可遍历、请求路径异常、可遍历下载文件、未鉴权、鉴权凭证脆弱、明文密码传输、登录页面存在账号密码、JWT 无签名算法、JWT 弱秘钥、账号名可枚举等 50+弱点识别规则；展示弱点 ID、弱点等级、应用名称、弱点名称、弱点类型、弱点状态、处理意见、API 标签、请求方法、单次返回最大数据量、访问域、部署域、返回类型、终端类型、最近活跃时间、首次发现时间等详细信息。支持按照弱点名称、弱点类型、弱点等级、弱点状态、应用名称、访问域、部署域、请求方法、终端类型、返回类型分组展示弱点。支持基于应用、弱点名称、应用名称、弱点类型、弱点等级、弱点状态、弱点 ID、API 标签、终端类型、返回类型、访问域、部署域等维度筛选弱点清单。支持手动新增弱点规则，新增包含 API、弱点、弱点等级、弱点特征、弱点描述、整改建议。并提供手动添加 Req_Raw/Rsp_Raw 样例和样例选择两种模式，选中匹配的样例接口。
风险发现能力	风险发现	▲支持风险识别，可按照数据泄露类、Web 攻击类、账号安全类进行分类管理。（投标人提供功能截图并加盖供应商公章）
		系统内置 10+风险策略，识别 API 接口异常行为风险。覆盖数据泄露类、Web 攻击类、账号安全类，包含 IP 访问次数异常、IP 执行参数遍历、Session 多终端访问、异常请求查询敏感数据、IP 执行翻页遍历、短信炸弹、验证码爆破、Web 攻击、IP 使用多账号、账号暴力破解、IP 高频撞库、账号异地登陆等。提供详细风险描述、风险状态、涉及数据标签等信息。提供详细的风险证据样例，包含采样证据、关联日志，并可查看证据样例，对涉及的敏感数据内容进行高亮展示。可基于风险证据样例，直接复制样例，便

		于风险验证确认。支持手动新增风险规则，新增包含风险名称、风险等级、风险类型、风险规则描述、风险主体、生效 API/应用、风险周期，风险指标等。风险指标覆盖访问次数、去重访问域数、去重 IP 数、去重省份数、去重终端数、去重文件数、请求关键字、返回状态码、返回长度、访问终端、IP 网段、Referer、操作时间范围、操作日期范围等。
数据解析能力	账号解析	支持多种账号解析提取方式，包含登陆认证提取、简单账号提取、SSO 认证提取的账号解析；支持登录认证提取，可提取账号字段、密码字段、登录凭证字段、登录成功判定字段等。支持简单账号提取，可自定义提取账号字段。支持 SSO 认证提取，可自定义提取账号字段、密码字段、登录凭证字段、Ticket、登录成功判定字段等。支持账号解析配置导入/导出，导入支持追加去重和覆盖方式导入。
数据审计	审计溯源	支持数据溯源、主体溯源、待离职人员审计、特权账号行为审计、资产与弱点离线审计等多种溯源场景。数据溯源：可基于敏感数据内容进行溯源，溯源结果包含关联日志条数、聚焦 IP、账号、API 个数，展示详细的溯源日志清单，支持导出，并可基于已建立数据溯源任务补充新数据溯源和创建主体溯源任务。
	资产与弱点离线审计	支持心间资产与弱点离线审计任务，可基于资产数据，覆盖 API 标签、API 状态、请求数据标签、返回数据标签、访问域等。可基于弱点数据，覆盖弱点名称、弱点状态、弱点等级生成报告。报告以 Excel 格式输出，支持下载后查看。
过滤配置	流量过滤	▲可通过规则、插件进行过滤，新增过滤规则名单，过滤方式包含：应用、API、目的 IP、请求方法、请求 UA、响应状态码、响

		应内容。（投标人提供功能截图并加盖供应商公章）
系统配置	数据开放	支持 syslog、kafka、邮件等多种方式同步数据，支持同步 API 清单、应用清单、弱点清单、风险清单、审计日志数据内容。同步内容可自定义选择新增数据或全量数据。同步格式包含内置格式、自定义格式。同步范围可选择应用、API 标签、访问域、自定义字段。同步规则可配置与或非任意组合。
	系统插件	系统内置扫描流量插件、脆弱性插件、API 标签插件、流量过滤规则插件。流量过滤规则插件包含非法 URL 请求过滤、无效域名过滤、响应内容不匹配过滤_Handler 使用、自定义 404 界面过滤_Handler 使用等插件。API 标签插件包含：注册 API、数据采集 API、短信验证码发送 API、人机访问 API、URL、重定向 API 等。脆弱性插件包含：JWT 弱密钥、请求权限参数可控、任意文件读取、请求路径异常、配置文件泄露、未鉴权等。扫描流量插件包含：log4j 攻击、PHP 异常参数攻击、异常文件上传流量、工具请求、xxe 漏洞利用攻击等。覆盖的插件不少于 80+。支持上传自定义插件内容。
	系统分权管理	支持基于资产权限、菜单权限、数据权限进行账号的权限定义，定义好的账号只能访问权限内的内容；支持自定义账号分组名称、分组描述；支持配置分组的资产访问权限；支持资产访问权限按照应用分配，支持指定应用、部署域、应用部门。支持系统管理员权限，历史分组删除；
	系统监控	无需登录系统后台，在前端 Web 界面可展示系统 CPU、内存、磁盘等使用情况。支持展示系统硬件配置信息，包含 CPU、内存、磁盘

		空间等。支持对机器启动时间、系统启动时间、机器运行时长、系统运行时长进行监测。可在系统 Web 界面执行 ping、telnet、ps aux、lsblk、df -h 等常见系统诊断命令。

数据库防火墙系统

类别	指标项	详细参数
性能	性能指标	吞吐量峰值不低于 20000 条 SQL/秒；并发连接数不低于 4000,时延≤3ms；不限制实例数。
部署方式	部署模式	支持代理模式，可代理数据库，实现系统采集到数据库流量；
数据库支持	数据源支持	支持传统关系型数据库，如:SQL Server、MySQL、Oracle、Sybase、DB2、Informix、PostgreSQL、MariaDB 的安全防护；
		▲支持内存数据库 HANA、Redis、Caché等特殊应用场景下的数据库安全审计；支持国产化数据库，如：DM（达梦）、LibrA、GaussDB、GBase 的安全防护；（投标人提供功能截图并加盖供应商公章）
		支持 IPv4/IPv6 网络环境流量的防护；
访问控制	控制模式	支持中断会话：对需要阻断的访问，中断数据库连接；拦截语句：对需要阻断的访问，返回防火墙的错误提示信息，当前语句被拦截后，该会话不中断；
数据防护	安全防护能力	▲支持基于嗅探技术寻找发现网络环境中存在的数据库资产，简化操作，实现数据库资产梳理；（投标人提供功能截图并加盖供应商公章）
		支持对操作时间、SQL 语句、执行结果、返回结果集、影响行数、执行时长、数据库用户名、实例名、源/目的 IP、源/目的端口、

		源/目的 MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、会话 ID 等 15 个条件以上进行审计；
		支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计以及阻断；
		支持基于 SQL 语法解析实现 SQL 操作的风险识别能力，非正则方式模糊匹配；
		▲支持拦截指定数据库对象的 ALTER TABLE、ALTER TABLESPACE、DROP DATABASE、DROP TABLE、DROP TABLESPACE、DROP USER、TRUNCATE 等高危操作行为，支持数据库权限变更行为管控；（投标人提供功能截图并加盖供应商公章）
安全策略配置	安全防护策略	▲内置安全特征库和审计规则库不少于 300 条，如 SQL 注入攻击、跨站脚本攻击、账号提权、导表导库等；（投标人提供功能截图并加盖供应商公章）
虚拟防护	虚拟补丁	▲支持针对利用已公开的数据库漏洞攻击行为进行拦截的虚拟补丁功能；（投标人提供功能截图并加盖供应商公章）
数据保护	敏感数据防护	支持根据时间、保护对象、源 IP 的维度对业务环境中敏感数据进行敏感数据统计、敏感数据访问热度统计及分析、敏感数据访问趋势及分析
产品描述	产品描述	针对数据库管理和运维安全的数据安全产品，通过访问控制、特权账户隔离、权限管控多种技术手段实现对运维人员操作行为的全面管控和审计。

数据防泄漏系统

类别	指标项	8 详细参数

软件授权	软件授权	支持终端授数量≥200 个；网络监测流量≥500M；
终端防护	上传管理	▲支持 QQ、TIM、WeChat 对话框的消息上传至 syslog 服务器，能够获取消息内容、发送方/接收方昵称（备注名称）、群/讨论组组名。（投标人提供功能截图并加盖供应商公章）
		对 QQ、TIM、飞鸽、飞秋等即时通讯软件上传文件的行为进行监控并识别上传的附件中是否包含敏感信息。
	应用程序管理	支持禁止运行外接设备上 exe 文件。
		支持应用黑白名单，白名单内的应用程序访问敏感文件不做处理，黑名单内应用程序访问敏感文件，支持监控审计或阻断；阻止通过修改进程名绕过黑白名单。
	打印控制	支持打印敏感内容监控、支持打印敏感文件添加水印功能。
	GIT 服务监控	支持终端只能向指定 git 服务器上传代码，向非指定 git 服务器上传代码阻断。
	敏感文件批量外发审批	▲可以选择单个或批量敏感文件，申请临时外发许可。同时支持右键菜单和气泡提醒窗口快捷进入审批界面。管理员可以修改外发申请的外发时间段和次数，也可以进行二级审批。外发申请批准后，可在批准的时间段和外发次数内外发指定的敏感文件。（投标人提供功能截图并加盖供应商公章）
	终端卸载管理	支持通过管理平台对在线终端进行卸载、禁用。
	终端数据发现	支持扫描本地文件，支持审计上传事件。
	响应方式	▲支持根据策略制定响应动作。响应动作包括：审计、发送电子邮件通知、记录到 Syslog 服务器、添加注释、设置状态、设置属性、

		限制事件数据保留、上传文件、加密、上传事件 LOG 文件、阻止、提示告警、标注分类分级（投标人提供功能截图并加盖供应商公章）
	客户端保护	▲禁止非授权用户强行终止代理的运行；禁止非授权用户强制取消代理在系统启动时自动加载；禁止非授权用户强制卸载程序；（投标人提供功能截图并加盖供应商公章）
网络敏感数据传输监测	软件敏感信息监测	▲对 QQ、TIM、飞鸽、飞秋等即时通讯软件上传文件的行为进行监控并识别上传的附件中是否包含敏感信息。（投标人提供功能截图并加盖供应商公章）
	网站监控	对通过 HTTP 发往豆丁文库、道客巴巴等的行为进行监控并识别出上传附件中是否包含敏感信息。
	邮件监控	对通过 HTTP 协议，yeah、163/126、阿里邮箱、新浪、139 邮箱发送邮件支持邮件标题、正文、附件的监控审计。
	论坛监控	对通过新浪微博、腾讯微博、各大贴吧、论坛传输文件的行为进行监控并识别出上传附件中是否包含敏感信息。
	邮件信息监控	对 webmail 的的发件人、收件人、抄送人和密送人全部展示
	邮件协议监控	对通过邮件客户端采用 pop3、imap 方式下载的邮件进行监控和识别
	传输协议监控	对通过 SMB 上传/下载、telnet、FTP 敏感文件的行为进行监控和识别

市财政局信息化日常驻场运维保障服务技术要求：

1) 提供工作日 5*8 小时驻场服务

2) 驻场工作人员手机需 24 小时保持畅通，遇到问题及时响应

3）重大活动和重大节日等保障时，需驻场配合保障。

1.3 服务标准：详见采购文件。

1.4 补充条款：合同签订后，供应商履约期间未经采购方书面同意，不得擅自更换项目组人员。

二、合同金额

2.1 本合同金额为人民币（大写）：捌拾壹万陆仟元整（¥816000）。

2.2 本合同价款包含所有乙方提供合同约定产品和服务的报酬及乙方提供合同约定产品和服务所支出的必要费用，甲方在上述合同价款之外不再向乙方支付其他任何费用。

三、技术资料

3.1 乙方应按采购文件规定的时间向甲方提供有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同产品和服务或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付标的的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 本合同不收取履约保证金。

七、合同转包或分包

7.1 本合同范围内产品或服务，应由乙方直接供应，不得转让他人供应或部分分包给他人供应。

7.2 如有转让和未经甲方同意的分包行为，甲方有权终止合同。

八、服务时间

8.1 服务时间：合同签订之日起一年。

九、合同内容的交付

9.1 交 付 期：合同签订之日起一年。

9.2 交付方式：项目需求单位指定方式。

9.3 交付地点：项目需求单位指定地点。

9.4 乙方应保证合同标的安全运达甲方指定地点，合同标的在交付甲方前发生的风险均由乙方负责。合同标的涉及包装的应符合《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的规定。使用说明书、质量检验证明书等（如有）一并提交甲方。

9.5 乙方在合同标的交付甲方 48 小时前通知甲方准备接收。合同标的在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方已送达。

十、合同款支付

10.1 付款方式：合同签订，服务人员进场后支付合同总价的 50%，服务满一个月，并出具服务报告，支付合同总价的 45%，服务期满验收合格后支付合同总价的 5%。

乙方收款信息如下：

户名:江苏移动信息系统集成有限公司

开户行：中国银行南京市云锦路支行

账号:479361758530

10.2 当采购数量与实际使用数量不一致时，乙方应根据实际使用量提供产品和服务，合同的最终结算金额按实际使用量乘以中标单价计算。

十一、税费

11.1 本合同执行中相关的一切税费均由乙方负担。

十二、质量保证及售后服务

12.1 乙方应按采购文件规定和响应文件承诺的性能、技术要求、质量标准向甲方提供产

品或服务。

12.2 乙方提供的产品或服务在服务期内因其本身出现质量问题，根据实际情况，经双方协商，可按以下办法处理：

（1）更换：由乙方承担所产生的全部费用。

（2）合同终止处理：合同终止，乙方退还甲方支付的合同款，同时承担由此产生的全部费用，甲方不承担任何产生费用。

12.3 如在使用过程中发生质量问题，乙方在接到甲方通知后 48 小时内到达甲方现场。

12.4 在服务期内，乙方应对产品或服务出现的质量及安全问题负责处理解决并承担一切费用。

十三、项目验收

13.1 甲方依法组织履约验收工作。

13.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

13.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

13.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

13.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时间、验收标准见采购文件验收内容。验收时，甲方按照采购合同的约定对每一项技术、商务要求的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

13.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方

式等适用《中华人民共和国民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十四、违约责任

14.1 甲方无正当理由拒收的，甲方向乙方偿付拒收标的总额 百分之五 的违约金。

14.2 甲方无故逾期验收和办理合同款支付手续的，甲方应按逾期付款总额每日 万分之五 向乙方支付违约金。

14.3 乙方逾期交付合同标的的，乙方应按逾期交付总额每日 千分之六 向甲方支付违约金，由甲方从待付合同款中扣除。逾期超过约定日期 10 个工作日 不能交付的，甲方可解除本合同。乙方因逾期交付或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总额 百分之五 的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

14.4 乙方交付的产品或服务不符合采购文件规定标准、乙方响应文件承诺及国家有关质量标准的，甲方有权拒收，乙方愿意更换但逾期交付的，按乙方逾期交付处理。乙方拒绝更换的，甲方可单方面解除合同，并由乙方赔偿由此造成的甲方全部损失。

十五、不可抗力事件处理

15.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同的，则合同履行期可延长，其延长期与不可抗力影响期相同。

15.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

15.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十六、解决争议的方法

16.1 甲乙双方因合同签订、履行而发生的一切争议，应通过友好协商解决。如协商不成，按下列第（2）种方式解决：

（1）向连云港仲裁委员会申请仲裁。

（2）向合同签订地法院起诉，合同签订地在此约定为连云港市。

十七、保密条款

17.1 未经甲方的事先书面批准，乙方不得以任何形式或任何方式将实施过程中接触到的信息和/或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得复制、泄漏或遗失。乙方亦不得依据保密信息，就任何问题，向任何第三方做出任何建议。

17.2 本保密条款在双方合作项目变更、解除、终止后十年内依然有效。本保密协议效力不因双方合作项目主协议的无效、撤销或变更而改变。甲方保留在甲方认为必要的情况下收回所提供的保密信息及其使用权的权利。

17.3 如任何一方违反本协议，违约方应按照《中华人民共和国民法典》的相关规定承担违约责任，另一方有权根据其违反的程度以及造成的损害后果要求对方赔偿因此遭受的损失

3002

十八、合同生效及其他

18.1 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

18.2 本合同未尽事宜，遵照《中华人民共和国民法典》、《中华人民共和国政府采购法》有关条文执行。

18.3 本合同正本一式 陆 份，具有同等法律效力，甲方执 肆 份、乙方执 贰 份，甲方报一份至政府采购监督管理部门。

甲方：连云港市财政局

地址：连云港市海州区海连中路 99 号

法定代表人或授权代表：

联系电话：

乙方：江苏移动信息系统集成有限公司

地址：南京市虎踞路 59 号

法定代表人或授权代表：

联系电话：

签订日期：2025 年 11 月 24 日