开封市“一道墙”数字政府安全运维能力支撑服务项目安全集成实施服务合同

（项目编号：汴财招标采购-2026-38-3）

甲方（采购人）：开封市行政审批和政务信息管理局

住所地：开封市民之家6楼东头向北6015

联系人：刘荫

联系电话：0371-22911919

乙方（中标人）：开封市新唯天电子有限公司

住所地：开封市宋城路129号

联系人：赵云云

联系电话：18637807690

根据《中华人民共和国民法典》《中华人民共和国政府采购法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，结合本项目招标文件、中标通知书及乙方投标文件，甲乙双方本着平等互利、诚实信用的原则，经协商一致，签订本合同。

第一章 项目服务内容与目标

第一条 项目服务内容

本项目为交钥匙服务项目，乙方负责完成数字政府安全运营平台定制开发、省局接口对接开发、配套安全产品部署、边界防火墙替换、系统联调测试、验收交付及三年免费运维服务等全流程工作，实现资产、情报、监测、预警、考评、联动、响应、分析、态势感知等核心能力，全面提升开封市数字政府安全防护与运营水平。具体服务内容、技术参数及功能要求详见本合同附件一《安全集成实施服务内容及技术要求》。

第二条 实施范围及要求

覆盖开封市数字政府安全运营平台开发、省局接口对接、配套安全产品部署、边界防火墙替换及三年运维服务。项目实施须符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）、《政务云安全规范》（GB/T 31167）、《信息安全技术 信息系统安全工程管理要求》（GB/T 20261）等国家及行业现行标准；合同履行期间标准更新的，按最新版本执行。

第二章 服务期限与实施

第三条 服务期限

总服务期限为合同生效之日起至三年运维期结束之日止。其中，实施开发期及试运行期不计入三年运维服务期，三年运维服务期自项目正式验收合格次日起计算。

平台开发与产品部署实施周期：合同生效后90个工作日内完成平台开发、产品到货、部署调试、联调测试，进入试运行阶段。

试运行期为30个日历日。试运行通过标准为：系统可用性≥99.9%，重大故障为零，所有功能指标符合附件一技术参数要求，且连续稳定运行满30日。试运行期满后，由甲方组织验收小组依据本合同及附件约定进行正式验收；验收不合格的，乙方应在5个工作日内完成整改并申请复验，复验仍不合格的，甲方有权解除合同并要求乙方承担违约责任。

第四条 实施要求

（一）乙方须制定详细的项目实施方案、进度计划，明确各阶段里程碑、责任人与交付成果，经甲方确认后执行。

（二）实施过程中严格遵守甲方机房管理、网络安全、数据安全相关制度，所有操作履行审批流程，严禁越权操作。

（三）上线操作须在甲方监督下进行，提前制定回滚方案，避开业务

高峰期，避免影响现有业务系统正常运行；操作失败须在30分钟内启动回滚，恢复业务正常状态。

（四）项目实施完成后，向甲方移交全套技术文档、管理手册、账号密码、原厂授权文件等全部资料。乙方移交的基于本项目所开发的源代码必须是完整未经加密的、可独立编译和部署的版本，并附带详细的编译说明、依赖库清单及数据库脚本；若项目中包含第三方商业软件或开源组件，乙方应提供合法的授权许可、二进制文件及必要的配置脚本，并确保甲方可独立部署和使用。甲方有权委托第三方机构对源代码及交付物进行完整性验证，若无法编译、运行或不符合授权要求，视为未完成交付，乙方应承担逾期交付违约责任。

（五）涉及功能范围、技术方案、工期、成本的任何变更，乙方须提交书面变更申请，说明变更内容、原因、对工期的影响，经甲方书面审批后方可实施；未经甲方确认，乙方不得擅自变更项目内容。

（六）乙方应建立项目风险台账，识别进度、质量、安全、合规等各类风险，制定应对预案；重大风险须第一时间向甲方书面报告。

第三章 合同价款与支付

第五条 合同总价

本合同总价款为人民币（大写）：**壹佰叁拾捌万陆仟元整（￥1,386,000）**。每年服务费用：肆拾陆万贰仟元整（**￥462,000**）。该价款包含硬件设备采购费、软件正版授权费、平台定制开发费、省局接口开发费、部署实施费、测试验收费、三年运维与升级服务费、技术培训费、备品备件费、运输保险费、税费及合同履约期间所有不可预见费用。合同履行期间，无论市场价格波动、政策调整或其他因素变化，合同总价均不作调整，甲方无需支付合同外任何费用。

第六条 付款方式

（一）付款周期：本合同服务费每6个月支付一次，共支付6次。每次支付金额为合同总金额的1/6，即人民币贰拾叁万壹仟元整（￥231,000.00）。每期款项的支付须以该服务周期届满且甲方考核合格为前提；若当期考核不合格，甲方有权暂停支付直至乙方整改合格，或按本合同第九章违约责任相关约定扣除相应费用后支付剩余款项。

（二）付款条件：每6个月服务周期届满，乙方须提交对应阶段成果证明材料及等额正规发票，甲方审核通过后15个工作日内完成支付。由于乙方提供的正式发票不合格而引起的一切责任（包括商业责任和法律责任）和损失由乙方承担。

（三）支付方式：银行转账。

（四）支付信息：

开户名称：开封市新唯天电子有限公司

银行账号：4100 1555 5220 5020 0900

开户银行：中国建设银行股份有限公司开封经济新区支行

（五）支付变更：乙方开户银行、账号等如有变更，应在本合同规定的付款期限前15天，以书面方式通知甲方。如未按时通知或通知有误而影响支付结算，乙方应承担相应责任。

第四章 双方权利与义务

第七条 甲方权利与义务

（一）有权对项目进度、质量、人员进行全程监督，提出需求变更与整改意见，对各阶段成果进行审核确认。

（二）提供项目所需的机房环境、网络条件、基础数据、业务系统对接支持，协调内部及第三方单位配合测试验收工作。

（三）按合同约定及时支付合同款项。

（四）不得要求乙方从事违反网络安全法律法规及保密规定的操作。

（五）组织项目各阶段评审、测试与最终验收工作。

第八条 乙方权利与义务

（一）严格按照招标文件与合同要求完成平台开发、产品部署、接口对接与实施交付，对项目整体质量、工期、安全负总责。

（二）组建专业稳定的项目团队，确保核心开发、实施人员全程在岗；人员变更须提前履行审批程序。

（三）保证提供的所有硬件设备为全新原厂正品，软件具备合法完整授权，符合国家相关标准与招标文件要求；提供原厂质保与售后服务。

（四）按约定提供技术培训，确保甲方操作人员、管理员能够独立操作、进行日常管理与处置常见问题。

（五）提供三年免费运维与技术支持服务，保障平台及设备稳定运行。

（六）对项目涉及的所有政务数据、系统信息、技术资料严格保密，严格遵守甲方保密管理规定。

（七）负责协调产品原厂、第三方厂商的技术支持，解决项目实施与运维中的技术问题。

（八）实施过程中采取有效措施保护甲方现有设备、系统与数据，因乙方操作造成损坏、丢失的，承担全部赔偿责任。

（九）按约定及时提交各类项目文档、报告与成果，确保文档真实、完整、规范。

第五章 项目团队管理

第九条 人员配置要求

（一）项目团队包含：项目经理、平台开发工程师、安全运维工程师，驻场人员不少于2人，各岗位职责清晰、互为补位。

（二）项目负责人须具备项目管理经验，持有项目管理、安全运维相关认证。

（三）核心开发人员须具备3年以上安全运营平台、政务信息化系统开发经验，熟悉政务云与电子政务外网架构。

（四）乙方可根据项目进度动态增派人员，确保工期与质量目标达成。

第十条 人员管理

（一）乙方不得随意更换项目负责人及核心技术人员；确需更换的，须提前15个工作日书面通知甲方，替换人员资质不得低于原人员标准，经甲方同意后方可更换。

（二）驻场运维人员考勤与甲方作息时间保持一致，请假须提前报备并安排顶岗人员。

（三）甲方有权要求乙方更换不胜任工作、违反管理制度的人员，乙方须在3个工作日内完成更换。

（四）乙方负责其工作人员的安全管理。乙方工作人员在履约过程中发生安全事故的，由乙方依法承担相应责任；因乙方或其工作人员过错造成甲方或第三人人身、财产损失的，由乙方承担赔偿责任。

第六章 故障响应与运维服务

第十一条 服务时限承诺

（一）故障分级标准：

- 一级故障（重大）：平台核心功能瘫痪、大面积业务中断、存在数据泄漏或安全事件风险。
- 二级故障（较大）：部分功能模块异常、非核心业务受到影响，可通过备用方式临时保障。
- 三级故障（一般）：局部功能瑕疵、界面显示异常，不影响核心业务运行。

（二）响应与修复时限：

➢ 一级故障：7×24 小时即时响应，技术人员 2 小时内到达现场，4 小时内恢复核心功能

➢ 二级故障：工作时间 10 分钟内响应，技术人员 4 小时内到达现场，8 小时内修复

➢ 三级故障：工作时间 30 分钟内响应，24 小时内完成修复

提供 7×24 小时技术支持热线，接到报修后立即响应；远程无法解决的故障，技术人员按上述时限抵达现场处置。

（三）故障处置完成后，乙方须在 24 小时内提交书面故障分析报告，说明故障原因、处置过程、整改措施及预防方案。

第十二条 运维服务内容

（一）服务期内免费提供平台功能优化、bug 修复、规则库升级、版本迭代服务；规则库与威胁情报常态化更新，安全策略按需优化。

（二）日常运行监控：对平台、配套设备运行状态进行 7×24 小时监测，每日生成运行简报，异常告警即时处置。

（三）季度健康巡检：每季度对平台、安全设备、服务器、存储进行全面健康检查，涵盖性能指标、安全策略、数据备份、日志审计等内容，出具正式巡检报告与优化建议。

（四）数据备份服务：定期协助甲方完成平台配置数据、业务数据备份，每半年开展 1 次备份恢复演练，确保备份数据可用。

（五）知识库建设：建立项目问题知识库，对常见问题、故障处置流程、操作规范进行整理更新，向甲方开放查阅权限。

（六）配合甲方完成与其他政务系统的对接适配，提供技术支持。

（七）重大敏感时期、重要会议活动期间，按甲方要求提供专项安全保障与驻场支持。

第七章 保密与信息安全

第十三条 保密义务

（一）乙方及所有项目人员对项目开发、实施、运维过程中接触的所有政务数据、业务信息、系统架构、安全策略、技术资料等负有永久保密义务。

（二）未经甲方书面同意，不得复制、留存、泄露、向第三方提供任何相关信息，不得利用相关信息从事与本项目无关的活动。

（三）乙方须与所有参与项目人员签订保密协议，并向甲方备案。人员离职前须完成资料交接与数据清理。

（四）乙方须定期对项目人员开展保密教育与考核，确保所有人员知悉保密义务及违规责任。

（五）保密义务不因合同终止、解除而失效，保密期限为永久。

第十四条 信息安全责任

（一）乙方运维操作须符合政务信息系统安全管理规定，严格执行操作审批流程，严禁越权操作。

（二）因乙方原因造成数据泄露、系统中断、网络安全事件的，乙方须承担全部法律责任及经济损失。

（三）运维操作全程留痕，操作日志至少留存6个月，重要操作须进行屏幕录制或安排双人旁站监督。

（四）因乙方原因引发网络安全事件的，乙方须立即启动应急预案，承担全部应急处置费用，并按相关规定承担行政及法律责任。

第八章 知识产权

（一）本项目实施过程中产生的工作成果（包括但不限于定制开发的数字政府安全运营平台、功能模块、源代码、目标代码、技术文档、数据、专利、著作权等）的知识产权均归甲方所有。

（二）乙方为本运维项目提供的硬件设备及配套软件相关知识产权归

时超过10次的，甲方有权解除合同，解除合同的通知自送达对方之日起生效。因乙方原因造成业务中断或安全事件的，乙方应赔偿甲方全部损失（包括但不限于直接损失、数据恢复费用、第三方评估费用、行政罚款及对第三方的赔偿等）。

（四）乙方发生以下情形之一的，甲方有权立即解除合同并要求乙方支付合同总金额20%的违约金，若违约金不足以弥补甲方损失的，乙方还应赔偿甲方的全部损失（包括但不限于行政罚款、对第三方的赔偿、律师费、诉讼费、重新采购成本等）：（1）发生重大网络安全责任事故（包括但不限于数据泄露、被上级通报批评、造成不良社会影响、被监管部门行政处罚等）；（2）擅自转包、分包本项目；（3）驻场人员资质造假或未经甲方同意擅自更换核心人员超过2人次；（4）泄露甲方敏感数据或违反保密义务；

（五）甲方有权直接从当期应付合同款项中抵扣。

第十章 不可抗力

（一）因地震、台风、水灾、战争、重大公共卫生事件等不能预见、不能避免且不能克服的不可抗力事件，导致一方不能履行合同的，受影响方应及时通知对方，并在15日内提供有效证明。

（二）受不可抗力影响的一方须采取合理措施减少损失扩大，未及时采取措施导致损失扩大的，扩大部分责任由该方自行承担。

（三）根据不可抗力影响程度，双方协商决定部分免除、全部免除责任，或延期履行、解除合同。

（四）不可抗力事件结束后3个工作日内，受影响方须向对方通报恢复履行计划，协商后续履约安排。

第十一章 合同的变更、解除与终止

（一）本合同的变更、补充须经双方协商一致，签订书面补充协议，

（二）本合同未尽事宜，参照招标文件、中标通知书及乙方投标文件执行。

（三）本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

（四）本合同自双方法定代表人或授权代表签字并加盖公章之日起生效。

（五）本合同载明的地址、联系人为双方法定送达地址与联系人，任何书面通知按该地址寄送或发送至指定邮箱，即视为有效送达；地址变更须提前3个工作日书面通知对方，否则承担送达不能的责任。

（以下无正文）

甲方（盖章）：开封市行政审批和政务信息管理局

法定代表人/授权代表（签字）：_____

日期：2026年8月28日

乙方（盖章）：开封市新唯天电子有限公司

法定代表人/授权代表（签字）：_____

日期：2026年8月28日

附件一

安全集成实施服务内容及技术要求

一、数字政府安全运营平台功能模块

（一）资产信息管理服务

1.包含单位管理、设备管理、业务系统管理、开放端口管理和应用资产管理。

2.单位管理支持单位名称、类型、省份、分组、是否重点、单位性质等基础信息管理。

3.设备管理支持设备所属单位、类型、IP、安全区、风险值、操作系统、责任人等属性管理。

4.业务系统管理支持统推系统下发、自建系统信息收集。

5.开放端口管理支持全网开放端口信息统计与管理。

6.应用资产管理支持全网应用资产信息管理，实现与省平台对接。

（二）威胁情报支撑服务

1.支持按IP、域名、文件HASH、邮箱、可疑URL等维度查询威胁情报，结合资产信息开展专项查询。

2.查询结果综合展示基本信息、威胁情报、开放端口、关联情报及来源信息。

3.实现威胁情报数据与省平台对接，支持情报导入、手工录入及第三方接口接入。

4.情报数据涵盖恶意IP、恶意样本、钓鱼网站、垃圾邮件、全球被黑网站等。

（三）分析检测支撑服务

通过动态采集流量行为日志，结合大数据算法与场景规则库，开展追踪溯源、告警、事件、脆弱性、威胁、资产多维度安全分析，实现一体化调查分析，输出威胁IP建档、资产画像、追踪溯源等成果。

（四）风险监测支撑服务

1.对下级单位告警信息进行统计分析，支持告警详情查看。

2.收集下级单位漏洞信息，支持漏洞详情查看。

3.统计全网威胁行为数据，包含事件类型、等级、数量、源目的IP、时间等。

（五）安全预警支撑服务

建立预警通报全流程机制，针对僵木蠕、通用漏洞等重大预警，覆盖事件排查、安全加固、漏洞复测全流程，实现“发现、验证、支撑、指导、闭环”管理。

（六）安全考评管理服务

1.设置管理、合规、资产、攻击事件、告警、漏洞、安全事件、应急响应等多类考核指标。

2.支持多维度考核设置，按周期对下级单位开展安全考核并统计结果。

（七）协同联动处置服务

1.联动漏洞扫描设备，实现脆弱性监测与资产漏洞展示。

三、配套安全产品部署产品明细

序号	设备名称	数量	技术参数	品牌
1	API 安全审计	1 套	（1）提供设备的 API 审计吞吐量 800Mbps。 （2）支持自定义日志保存配置，配置选项包含但不限于：不设置、保存包含风险事件的访问日志、保存包含敏感数据的访问日志、保存包含事件或敏感数据的访问日志、只保存同时包含敏感数据并触发事件的日志； （3）支持对请求和返回中传输的敏感数据类型进行识别，内置敏感数据识别规则至少包含身份证、手机号 、护照号码、港澳台身份证号 、外国人居留许可证等常见敏感数据类型。。 （4）支持通过内置策略或自定义策略识别接口属性并打标，属性标签类型包括但不限于：注册接口、数据查询接口、文件上传接口、文件下载接口、用户登出接口、短信发送接口、验证码发送接口、数据导出接口等； （5）支持对 IP、用户进行画像分析，展示指定时间范围内的访问关系、敏感数据获取量、文件下载数量、使用 IP 数量、访问域名数量、访问 IP 数量、请求量及趋势、请求域名分布、服务端 IP 分布、敏感数据流动趋势及数量、敏感数据流动类型等信息； （6）支持以域名、HOST、客户端 IP、用户、事件、标签、应用、为维度对数据流出情况进行多维度统计分析；透出统计信息包括但不限于敏感数据流动量及趋势图、敏感数据类型分布及数量、数据透出域名排行、数据透出 IP 排行、数据透出地域及网段分布、IP 获取量排行、敏感数据访问事件等信息；并支持跳转到详细事件访问审计日志； （7）支持基于完整 URL、服务端口、域名、路径、查询参数、状态、客户端 IP、请求或响应敏感数据类型、敏感数据数量、未鉴权 API 标签、URL 中包含密码、账号登录行为、弱密码检测结果等条件组合配置风险匹配规则； （8）通过 Web API 接口向外部系统传输 API 资产信息、检测到的威胁信息、脆弱性信息和风险事件、系统运行监控信息和审计日志。	昂楷

2	深度威胁检测	1套	（1）具备本地安全事件调查能力（非云端）。 （2）支持通过判定信息自动描述恶意攻击事件的相关轨迹信息，自动记录黑客攻击链条执行的所有操作。 （3）自动生成事件信息卡，用于安全事件溯源分析。 （4）具备威胁狩猎功能，自行关联相关程序，通过可视化威胁关联图，快速找出威胁程序的前后关联。 （5）支持禁止程序执行、主机隔离、远程进行对象删除、隔离文件、远程进行系统扫描、远程执行应用程序/命令、远程执行IoC扫描等响应措施，并支持将可疑文件进行远程提取或远程恢复。 （6）能够导入YARA规则，用于扫描端点上的对象。 （7）解决方案必须与威胁情报分析门户集成。	卡巴斯基KEDR
3	政务云安全管理服务	1套	（1）120个通用授权及三年规则库升级，支持多租户云架构，包含租户自助服务和集中运营管理功能，为租户提供自助服务门户，按需开通所需安全组件，对安全资源池内的租户账号和安全组件进行统一管理、集中监控。 （2）支持显示了云安全运营平台下的所有租户申请的安全实例信息，包含租户名称、实例类型、实例状态、区域、开通时间、是否过期等信息，并且可查询相应租户服务。 （3）支持对资源池平台内部安全网元的管理，可以上传网元文件，设置产品价格、详情介绍。 （4）支持扩展无代理的虚拟分布式防火墙，可灵活应对租户东西向的安全防护需求。。 （5）支持可视化的服务链编排能力，可以定义租户流量经过安全网元的路径顺序。 （6）支持安全实例申请，自动化创建、删除、操作配置、续费操作。续费支持手动续费和自动续费。租户可直接登录到安全组件管理页面，无需再次输入账号密码。 （7）支持通用授权点模式，需要进行租户数量、网元类型、网元数量的授权，租户才可正常使用。可以展示整体的授权点数，已使用授权点及剩余授权点。并可进行筛选查看指定网元的授权到期详情。 （8）支持监控云安全资源池平台运行状况，包括安装资源池物理机总数、物理机在线数、物理机离线数、整个资源池平台内存/CPU/磁盘使用率，各个物理机IP地址、状态、内存/CPU/磁盘使用率、网卡流量趋势。 （9）支持监控每个租户的网元信息，包含网元的CPU、内存、硬盘使用率及使用趋势、流入带宽、流出带宽。。 （10）支持监控云安全资源池整个系统的服务运行状况，包括虚拟化平台、运营平台、EDR安全管理平台的服务运行状况。 （11）支持自定义的形式配置到云安全管理平台，以产生满足条件的告警信息。同时支持指定时间段内，发现满足过滤器条件的事件累计发生次数超过规则设定的阈值时，表明出现了潜在危害，产生告警信息。支持指定告警级别	天融信