开封市豫正通平台项目合同

（项目编号：汴财招标采购-2026-36）

甲方（采购人）：开封市行政审批和政务信息管理局

住所地：开封市郑开大道与三大街交叉口市民之家

联系人：孟祎

联系电话：13140192575

乙方（中标人）：正数网络技术有限公司

住所地：河南省郑州市郑东新区金水东路39号中国河南出版产业园D座6-7楼

联系人：王振宇

联系电话：18638523332

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》《中华人民共和国个人信息保护法》等相关法律法规，结合本项目汴财招标采购-2026-36招标文件、中标通知书及乙方投标文件，甲乙双方遵循平等、自愿、诚信原则，经协商一致，签订本合同。

第一章 服务内容与技术标准

第一条 服务内容

乙方为甲方提供开封市豫正通建设，分别为应用系统、应用支撑系统、安全服务系统三大板块。全部内容清单如下：

1、应用系统：包含重点督办、应急指挥、领导批示、经济运行、委　局

直通、个人中心6个业务模块;

2、应用支撑系统：包含统一用户中心、督办事项填报平台、指标填报、接口聚合、监控管理、指标更新6个核心支撑模块;

3、安全服务系统：共计7项安全专项服务，分别为Web应用防护服务、日志审计服务、漏洞扫描服务、数据库审计服务、安全管理中心、威胁安全检测服务、安全认证服务。

具体服务内容、技术指标等要求详见本合同附件一《服务内容及技术要求明细》，该附件与招标文件、乙方投标文件共同构成本合同履行及验收依据。

第二条 技术标准

（一）乙方提供的服务符合国家、行业现行网络安全、政务信息化相关标准和规范。

（二）乙方使用的开发框架、运维工具、监测平台、第三方组件及商用软件，须为合法正版授权产品；维保期内须按规定完成版本升级、规则库更新与许可续期，严禁使用盗版、破解版或未授权开源衍生产品，由此引发的法律责任及经济损失由乙方承担，乙方承担赔偿总额不超过本合同价款。

（三）乙方所交付的系统、组件、工具须具备良好的兼容性、可扩展性与国产化适配能力，能够在国产CPU、操作系统、数据库、中间件环境下稳定运行。

第二章 合同履行期限

第三条 合同履行期限

乙方应于本合同生效之日起120日历天内完成项目全部开发工作并完成试运行，试运行期为30日历天。试运行期满，项目运行稳定、未发生影响业务正常使用的故障，乙方即可提交项目验收申请。本合同运维服务期限为1年，安全服务期限为3年，自项目验收合格之日起开始计算。

第三章 合同价款与支付

第四条 合同总价

本合同总价款为人民币（大写）：**壹佰肆拾叁万陆仟元整（¥1,436,000.00），增值税率6%，不含税金额：壹佰叁拾伍万肆仟柒佰壹拾陆元玖角柒分（￥1,354,716.97），增值税：捌万壹仟贰佰捌拾叁元零叁分（￥81,283.03）。**该价款包含人员成本、差旅费、耗材、保险、税费、培训、应急保障、售后服务等全部费用，甲方无需支付合同外任何费用。

第五条 付款方式

（一）付款方式：项目验收合格后，甲方向乙方支付至合同总价款的30%，即人民币（大写）：**肆拾叁万零捌佰元整（¥430,800.00）**。运维服务满半年无质量和服务问题，支付至合同总价款的60%，即人民币（大写）：**肆拾叁万零捌佰元整（¥430,800.00）**。运维服务满一年无质量和服务问题，支付至合同总价款的100%，即人民币（大写）：伍拾柒万肆仟肆佰元整**（¥574,400.00）**。

（二）资金来源：财政全额资金

（三）付款条件：

1.每个付款阶段，乙方提交付款申请、等额正规发票，甲方确认后，

及时会同财政部门办理合同履约款项拨付手续，将对应款项支付至乙方指定银行账户。乙方对财政资金拨付相关流程予以认可。

2. 乙方提交资料不完整或发票不合规的，相应期间付款期限不起算，甲方不承担逾期责任。

3. 由于乙方提供的正式发票不合规而引起的一切责任(包括商业责任和法律责任)及造成的损失由乙方承担。

（四）支付方式：银行转账。

（五）支付信息：

开户名称：正数网络技术有限公司

银行账号：3719 0811 9610 006

开户银行：招商银行股份有限公司郑州分行营业部

（六）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

第六条 甲方权利与义务

（一）有权对乙方工作进度、数据安全进行监督、检查与考核，对不符合要求的事项提出整改要求。

（二）向乙方提供项目所需的现有环境、系统资料、业务系统相关基础信息，配合乙方开展开发及运维工作。涉及账号、权限的，按最小必要原则授权。

（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国家法律法规、网络安全法律法规及保密规定的操作。

（五）负责审核乙方提交的重大操作、系统变更申请，按照内部管理流程予以审批。

第七条 乙方权利与义务

（一）严格按照招标文件、投标文件及本合同约定完成项目开发、提供运维服务，确保服务质量达到约定标准，保障项目 7×24 小时安全稳定运行。

（二）组建符合要求的项目团队，遵守甲方各项管理制度与保密规定，服从甲方工作安排。乙方应向甲方提供项目团队人员名单，签订保密承诺等材料，人员变更同步报备。

（三）在平台建设及运维服务全过程，建立规范完整项目档案，定期梳理编制项目工作总结报告，汇总阶段性工作开展情况、故障/问题情况、存在风险、整改情况及下期工作计划。报告经甲方确认后归档。

（四）在平台建设及运维服务全过程，对发现的安全隐患、故障风险及时向甲方书面报告，并提出整改建议。如发现网络安全事件、数据安全事件或个人信息泄漏情形的，应立即报告并采取应急处置措施。

（五）承担服务过程中因乙方操作不当、管理疏漏造成的设备损坏、数据丢失、安全事件的全部责任。

（六）不得转包本项目：未经甲方书面同意，不得分包。经甲方书面同意分包的，乙方就分包项目向甲方承担全部责任，分包方不得再次分包。

第五章 项目团队管理

第八条 人员配置要求

（一）项目团队总人数不少于5人，进入运维期后提供7×24小时远程运维保障。

（二）项目负责人须具备项目管理经验，其资历不得低于投标文件承诺标准。

（三）项目运维服务期满后，乙方须承诺在法定工作时间内，可以提供免费的技术指导和咨询。

第九条 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) 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。

(三) 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 服务质量

第十条 响应时效要求

（一）收到故障报修后，工程师须在10分钟内响应；一般故障须在30分钟内采取临时措施恢复业务运行，并在24小时内彻底修复；重大故障须在1个工作日内完成修复(含数据恢复时间)。如无法在上述时限内彻底修复，乙方须立即书面说明原因、预计修复时间及应急保障措施，经甲

方同意后方可延期。

（二）远程无法处置的故障，乙方须在 24 小时内调配技术人员到场维修。

（三）故障分级标准:

➢ 一般故障：影响业务用户数量＜20%；造成中断时间：＜0.5 小时，影响系统效率，使系统业务处理能力受到影响;

➢ 较大故障：造成系统影响业务用户数量：20%≤数量<50%；中断时间：0.5 小时≤时间<4 小时，明显影响系统效率;

➢ 重大故障：指造成系统长时间中断或局部瘫痪，影响业务用户数量≥50%；中断时间：≥4 小时；使其业务处理能力受到极大影响，系统关键数据的保密性、完整性、可用性遭到破坏;

（四）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。

第十一条 验收管理

（一）验收依据。本项目以本合同、招标文件、乙方投标文件、附件一《服务内容及技术要求明细》及双方书面确认的变更文件为验收依据。

（二）验收流程。乙方完成全部建设内容并试运行期满自检合格后，向甲方提交验收申请及交付物清单（含系统部署包、技术文档、操作手册、测试报告等）；甲方应在收到验收申请后 20 个工作日内组织验收，甲方逾期不组织验收且无书面异议的，经乙方书面催告后，甲方在另行确定的合理宽限期（如 15 个工作日）内仍无正当理由不组织验收的，方视为合格，运维服务期自动起算；验收合格的，双方签署验收报告，运维服务期

自动起算。验收不合格的，乙方应无偿限期整改并重新申请验收，整改期间不计入运维服务期，由此产生的费用及损失由乙方承担。

第七章 保密、信息与数据安全

第十二条 保密义务

（一）乙方及项目人员对服务过程中接触的政务数据、网络架构、安全策略、业务信息等信息负有保密义务。

(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)保密义务不因合同终止、解除而失效，保密期限为永久。

(四)乙方须与所有参与项目人员签订保密协议，并向甲方备案。人员离岗时应交还资料、注销权限并继续承担保密义务。

(五)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。

第十三条 信息安全责任

（一）乙方平台建设、运维操作须符合政务信息系统安全管理规定，严格执行操作审批与最小权限原则，严禁越权操作。

（二）乙方应安排具备专业能力的安全技术人员，按照国家网络安全等级保护相关要求及行业规范，对乙方交付的业务应用系统进行定期安全维护、漏洞扫描、渗透测试及安全检测；同时建立常态化安全防护机制，及时修复系统安全漏洞，确保项目安全稳定运行。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，不以合同价款为限。

（三）运维系统日志全程留痕，应用系统日志至少留存6个月并按等保要求备份，重要操作须进行屏幕录制或安排双人旁站监督。日志归甲方所有，乙方不得删除、篡改。

（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。

（五）乙方须保障本项目符合网络安全等级保护要求三级，乙方需配合甲方组织等保三级评测，等保测评费用由甲方承担。

第十四条 数据安全与个人信息保护

（一）本项目履行过程中采集、存储、处理、传输的全部政务数据及个人信息，其所有权、管理权归甲方（或有权机关）所有。乙方仅得在本项目目的范围内，按甲方指令进行处理，不得用于任何其他目的，不得擅自留存、使用、出售、向第三方提供或公开。

（二）乙方应依照《数据安全法》《个人信息保护法》落实数据分类分级、加密、访问控制、脱敏、审计等措施；处理个人信息应遵循合法、正当、必要和诚信原则，不得超范围收集，不得非法获取、泄露个人信息。

（三）未经甲方书面同意且未依法完成安全评估等程序，乙方不得将政务数据、个人信息传输至境外，不得委托、共享给任何第三方；服务期内及结束后均不得以任何形式向公共云平台、人工智能模型或第三方系统上传、投喂本项目数据。

（四）发生或可能发生数据泄露、篡改、丢失及个人信息安全事件的，乙方应立即采取补救措施，及时书面通知甲方，配合甲方履行报告、通知和处置义务，并承担由此产生的全部责任与费用，不以合同价款为限。

（五）合同解除、终止或交接时，乙方应按甲方要求完整返还、移交全部数据及副本，并从其所有设备、系统、介质中彻底删除，出具书面删除确认；甲方有权对返还与删除情况进行核查。

第八章 知识产权

（一）乙方为本项目专门开发、形成的系统功能、方案、文档及其他交付成果，其知识产权归甲方所有。乙方应在交付时一并提供完整部署包代码、技术文档及部署说明，并不得就上述成果向甲方主张任何权利。

（二）乙方保证提供的工具、软件、技术方案不侵犯任何第三方知识产权；如发生侵权纠纷，由乙方负责处理并承担全部责任、赔偿甲方因此遭受的全部损失。

（三）乙方交付的所有文档、报告、方案等成果，甲方有权无偿使用、复制、修改及内部分发，用于本单位管理及政务服务相关工作。

（四）乙方为履行本合同所使用的自有工具、软件，授予甲方永久的、非排他的、不可转让的免费使用权，使用范围包括本项目及后续相关政务信息系统的运维管理工作。该授权不因本合同的终止、解除或期满而失效。

第九章 违约责任

第十五条 甲方违约责任

（一）因甲方导致逾期支付合同款项的，每逾期 1 日，按应付未付金额的 0.01%向乙方支付违约金。

（二）甲方按规定完成资金申报手续，但因财政原因等非甲方主观原因，导致资金未能及时、足额拨付的，乙方应与甲方协商沟通，甲方持续跟进资金拨付进展，并及时向乙方同步相关情况。

第十六条 乙方违约责任

（一）乙方未按约定配置人员、人员资质不符合要求的，每发现1项向甲方支付合同总金额0.05%的违约金，并限期整改；逾期不改的，甲方有权解除合同。

（二）故障响应、处置超出约定时限的，每逾期1次支付2000元违约金，一般过失以合同价款为限；因乙方故意或重大过失、违反保密/数据安全/网络安全义务、侵犯第三方知识产权、人身损害及发生数据泄露、网络安全事件的，不设赔偿上限、不以合同价款为限。

（三）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5%的违约金，并赔偿甲方损失：

1、连续发生网络安全责任事故；2、泄露甲方敏感数据或违反保密、数据安全义务；3、因乙方原因导致核心业务连续中断超过24小时且乙方不能说明合理原因的；4.擅自转包、分包本项目。

（四）乙方违反保密义务或泄露甲方重要数据、信息的，须向甲方支付合同总金额10%的违约金；若违约金不足以弥补甲方损失的（包括但不限于行政罚款、对第三方赔偿、应急处置费用等），乙方应予补足。

（五）因乙方原因逾期完成本项目平台建设，每逾期1日按合同总金额0.01%支付违约金，累计违约金不超过总金额的5%；逾期超过30日的，甲方有权解除合同并要求赔偿损失。

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，补充协议与本合同具有同等法律效力。

（二）一方严重违约导致合同目的无法实现的，守约方有权书面通知解除合同。

（三）本合同全部解除条款适用如下规则：解除合同的通知，自送达对方之日起生效。

（四）合同期满，双方义务履行完毕，合同自动终止；如甲方有续约需求，可按政府采购规定办理后续手续。

（五）合同解除或终止后，乙方须在5个工作日内提交详细交接计划，并在20个工作日内完成全部工作交接，移交内容包括但不限于所有系统账号及密码、运维档案、配置脚本、未结工单、已知安全隐患清单、工具资料、备品备件等，配合甲方完成后续衔接工作。

（六）合同终止后，乙方仍须对服务期内已知的安全隐患履行告知义务，并配合甲方做好收尾处置工作。并按第十四条完成数据返还与删除。

第十二章 争议解决

因本合同引起的或与本合同有关的任何争议，双方先友好协商解决；协商不成的，任何一方均有权向甲方所在地有管辖权的人民法院提起诉讼。

第十三章 其他约定

（一）本合同附件为本合同不可分割的组成部分，与本合同正文具有同等法律效力。

（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）本合同一式陆份，甲方执叁份，乙方执叁份，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。

附件：1. 服务内容及技术要求明细

2. 中标通知书

（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10月22日

乙方（盖章）：正数网络技术有限公司

法定代表人/授权代表（签字）：

日期：2026年10月22日

附件 1

服务内容及技术要求明细

序号	系统板块	模块	技术要求
1	应用系统	重点督办	包含 PC 端和移动 APP 端两个入口。PC 端面向全体用户提供操作页面，承载重点交办、重点工作督办、好差事项、领导批示相关业务，可为督办牵头、承办、配合单位提供事项新建、反馈、申请、督办、审批、导出等操作，相关督办事项可在政务云完成全流程流转。市级具备录入权限的用户，可在 PC 端完成督办事项录入、反馈、延期申请、办结申请、下发督办通知、发黄牌警示，同时可开展信息报送录入、审核、呈批、呈阅工作。移动 APP 端重点面向市委市政府领导，在移动端展现各类重点督办事项的名称、具体内容、督办落实情况等信息，方便领导及时查阅并进行重要批示。
2		应急指挥	面向市领导提供信息查询能力，可快速调取应急指挥体系、应急处置方案、实时监测数据，配套视频语音交互功能，实现应急场景可视、可联；后台管理端支持工作人员维护指挥体系、应急方案基础信息。
3		领导批示	依托平台汇聚整合的数据支撑市级领导开展决策部署、工作安排、时效监督，完整复刻线下纸质批示流程，形成线上可视、可联、可办、可督的闭环流转机制；遵循 “豫正通” 分层分级规范，针对每位市级领导打造定制化操作界面，实现千人千面专属服务。
4		经济运行	整合展示全市生产总值、项目投资进度，汇总规模以上工业、固定资产投资、社会消费品零售、财政收支、进出口五大类经济指标，支持指标查看、关注、在线批示，便于领导统筹掌握全市经济动态。
5		委局直通	统一归集各委办局业务数据，按业务分类提炼核心指标，直观展示各单位牵头工作推进进度，覆盖指标调研梳理、系统对接、UI 设计、人工数据填报全流程；通过数据分析评估，实时呈现各委办局核心数据，方便领导实时掌握、督导各单位工作。覆盖市行政审批和政务信息管理局、林业、水利、财政、卫健委等全部委办局。
6		个人中心	为系统所有登录用户提供专属个人空间，支持修改个人资料、重置登录密码、查看与管理我的关注信息；可查询当前使用应用版本号，便于运维人员快速定位故障版本，统一开展应用版本管控。
7	应用支撑系统	统一用户中心	全域身份管理基础模块，归集全部委办局人员用户数据，统一管控角色、职务、部门权限体系。

8		督办事项填报平台	一体化督办任务管理载体，统筹各类工作任务跟踪落实，集成督办新建、任务办结归档、逾期智能分析、公务短信推送、统一通知中心、全局检索、督办通知下发等功能。
9		指标填报	统一管控全部业务指标，设定录入规范，可选指标录入格式（数字、文本等），为每项指标配置更新周期，超期未填报自动提醒对应单位经办人；对接委局各类业务接口时可设置数据采集周期，保障数据时效性。
10		接口聚合	接口采集模块对接市级数据共享交换中心，自动采集各委办局通过业务系统对接到数据共享交换中心的接口数据，可存入本地数据库或直接转发至用户使用。
11		监控管理	实现主机、数据库、中间件、业务应用全方位多维度监控；多渠道推送系统告警；统一采集、存储全量系统日志；支持批量化脚本执行、文件分发等作业管控。
12		指标更新	统一管控指标发布、数据预警机制，规避失真数据误导领导决策。
13	安全服务系统	Web 应用防护服务系统	硬件需求：搭载交流冗余电源模块，不少于 2 个 USB 接口、1 个 RJ45 串口、4 个千兆电口(支持 2 对 Bypass)、1 个接口扩展槽，HTTP 应用层吞吐量最低 800Mbps； 部署模式：支持透明串联、旁路路由回注、反向代理、镜像监听四种部署方式； 安全防护能力：网页盗链拦截、Cookie 安全管控、自定义敏感关键字；识别拦截恶意试探、撞库、暴力登录等违规访问；防御 SQL 注入、XSS 跨站、SSI 指令、Webshell、路径穿越、远程文件包含攻击；按国家 / 区域维度限制 IP 访问，抵御区域性网络攻击；阈值告警、请求量统计、应答分布统计多重扫描防护；留存完整原始攻击日志，可与安全管理中心平台联动。

14		日志审计服务	硬件需求：搭载交流冗余电源模块，不少于 2 个 USB 接口、1 个 RJ45 串口、1 个管理口（千兆电口）、6 个网络接口（千兆电口）、4 个千兆光口、1 个接口扩展槽位，4T 有效存储容量；不少于 60 个日志源接入授权，内置 1 个采集器； 日志采集：兼容 SNMP Trap / Syslog / ODBC / UDBC / WMI / FTP / SFTP 多类采集协议与接入方式； 日志处理：统一解析异构日志并完成范式化，强制范式化字段涵盖收发时间、账号、源目的地址/端口、操作行为、网络协议、设备信息等；新增日志类型仅修改配置文件即可适配，无需编码； 资产与分析：支持日志 IP 信息自定义资产资源并供规则引用；资产拓扑支持列表、拓扑双视图，向下钻取可分别查看资产独立事件、告警列表；支持基于时间、行为开展日志关联分析，生成事件拓扑图； 存储转发：支持多目标地址日志转发，原始日志 IP 信息不丢失；支持 NFS 共享扩容存储；内置交换机事件编码知识库、Windows / Linux 系统、MySQL / Oracle / SQL Server 数据库事件知识库，可查询各类事件说明。
15		漏洞扫描服务	硬件规格：配置 1U 设备，不少于 1 个管理口、1 个 RJ45 Console 口、2 个 USB 接口、4 个网络接口（千兆光口）、4 个千兆电口、1 个接口扩展槽位； 扫描性能：最大可扫描 IP 数量≥500 个，并发扫描 IP ≥60 个； 扫描覆盖范围：兼容 Windows、通用 Linux、麒麟、统信 UOS 系统，支持借助域管理员权限开展 Windows 域深度扫描；可检测漏洞总量≥190000 个；支持达梦、人大金仓、优炫、Oracle 等主流国产、国外数据库，数据库漏洞检测方法≥2600 种；适配 OpenStack、VMware、Docker 等虚拟化平台，虚拟化漏洞检测方法≥2600 种；支持 WPS、永中、用友等国产软件及大华、海康、等视频监控设备漏洞检测；支持 DNS 投毒、幽灵木马专项检测。 扫描策略：内置 20 套以上默认扫描模板（常规扫描、高危漏洞、云平台、虚拟化、视频设备扫描等）；提供面向漏洞市场应急响应的专属策略模板，支持自定义策略模板。

16		数据库审计服务	硬件需求：内存≥16G，硬盘≥2T，≥6 个千兆电口，≥4 个千兆光口，≥1 个接口扩展槽位，2 个 USB 接口，1 个 RJ45 串口；数据库实例数≥30 个； 数据库兼容审计：覆盖但不限于达梦、MySQL、Oracle、SQL-Server、人大金仓、高斯、MongoDB、Redis、Hive 等数据库审计； 数据库攻击审计：审计 SQL 注入、XSS、高危 CVE 漏洞利用、暴力口令、缓冲区溢出攻击；完整审计访问源主机、账号、SQL 执行耗时、操作成功 / 失败状态； 基线与敏感数据：自动构建账号、操作类型（SQL 模板）等数据库行为基线，异常操作实时告警；自动识别数据库、资源账号、表名，定位身份证、银行卡、密码等敏感字段，分级配置风险值评估泄露隐患；支持探测器、正则两种敏感数据识别方式； 告警与处置：可基于风险操作、SQL 注入、漏洞攻击、语句管理模块配置高 / 中 / 低三级告警规则，支持系统资源监控告警；按安全级别区分记录、告警处置动作，告警支持邮件、短信、Syslog、SNMP；通过模式匹配结合 SQL 注入特征库识别注入语句；高风险会话支持旁路阻断；支持姓名、身份证、手机号、银行卡、住址及自定义字段敏感掩码，防止审计日志敏感泄露；敏感数据大屏展示分级占比、访问分布、TOP5 账号 / IP、增删改插操作统计。
17		安全管理中心	硬件需求：搭建冗余电源、专用千兆硬件平台和安全操作系统，≥2 个 USB 接口、≥2 个千兆电口，24 个千兆光口，≥3 个接口扩展槽位，有效存储容量≥32TB； 日志解析：内置 300＋设备日志解析规则查看以及筛选，包括网络设备、安全设备、终端主机日志、数据库等； 威胁研判：自动判定失陷资产，输出攻击链、攻击流量、原始日志、PCAP 取证包，可关联查询同资产、同攻击者全部威胁事件； 态势可视化：综合展示全网安全总态势、威胁分布、漏洞脆弱性、环境感知、运维处置全维度数据；可视化统计人工事件状态、数量、自动化编排和响应的时长、数据量及任务数等数据； 闭环处置：支持对各类运维事件进行运维处置，包括但不限于提交研判人员进行分析、忽略、误报标记、加入白名单、生成报告、联动设备封堵处置等；可对 IP、域名等封堵，依托黑名单、流量牵引联动 WAF、防火墙等执行阻断；漏洞扫描结果自动生成处置工单，支持新增、待修复、已修复、已验证、单次忽略、永久忽略全状态闭环管理。

18		威胁安全检测服务	硬件性能：≥1 个管理口、≥6 个千兆电口、≥4 个千兆光口，≥1 个接口扩展槽，≥2 个 USB 接口；≥1 个 RJ45 串口；应用层吞吐量≥1000Mbps;最大并发会话数≥300 万；每秒新增会话数≥2 万；SATA 硬盘容量不低于 10T。； 采集检测能力：融合 IDS、WAF、威胁情报、全流量行为日志采集，对接第三方大数据平台；检测入侵攻击、Web 应用、恶意文件、弱口令、拒绝服务攻击；结合双向流量、元数据、原始数据包、研判模型深度研判攻击结果；具备本地授权、流量采集、元数据提取、流量存储功能；实时流量 PCAP 包全量存储用于取证追溯； 协议解析：深度解析并还原 TCP、UDP、SCTP、ICMPv4 / ICMPv6、VLAN、MPLS、HTTP、SSL、FTP、SSH、DNS、NGAP、GTP-U、MQTT 等常见通用、5G、物联网协议；自动化精准识别资产，包含设备类型、资产名称、操作系统、MAC、IP、端口等信息。
19		安全认证服务	部署兼容：支持虚拟化部署，适配政务云，兼容 X86、ARM 硬件架构，提供定制移动端 APP 加固 SDK；性能指标：每秒新建 SSL 连接≥5000/s，并发在线用户数≥200/s，可管理设备用户数≥1000； 客户端适配：Windows 7/8/10、OSX 10.12 及以上版本、Linux(Ubuntu 16 及其以上版本)、Android 5.0 及以上系统，移动端 SDK 可嵌入自有业务 APP； 风险访问管控：统计授权成功 / 失败次数、TOP 授权应用排名；展示终端在线总量、总终端数等；识别非工作时段登录、陌生终端、异地地址异常登录并告警；结合用户身份、终端状态、用户行为持续评估访问风险，支撑动态授权决策；分析访问时段、地理位置、操作行为，识别破解、异地、非注册终端异常访问行为； 精细化认证策略：按用户组、地理位置、访问时段配置认证规则，强制高危场景双因子认证；SPA 单包授权防护机制，未认证应用不可访问，外部扫描探测不到端口；网关静默全 TCP 端口防攻击，校验通过开放动态端口，端口策略可按需开关；支持 UDP 协议 SPA 单包授权验证。

附件 2

中标通知书



中标通知书（服务）

正数网络技术有限公司：

根据开封市行政审批和政务信息管理局开封市豫正通平台项目（项目编号：汴财招标采购-2026-36）招标文件和你单位于 2026 年 9 月 29 日提交的投标文件，通过公开招标方式，经评标委员会评审，现确定你单位为上述交易项目的中标人，主要内容如下：

项目名称	开封市行政审批和政务信息管理局开封市豫正通平台项目
项目编号	汴财招标采购-2026-36
合同价格（人民币）	小写：1436000 元 大写：壹佰肆拾叁万陆仟元整
合同履行期限	合同签订生效后 120 日历天完成项目全部工作。
服务期限	系统运维自项目验收合格之日起 1 年， 安全服务自项目验收合格之日起 3 年。
招标代理机构	开封市政府采购中心

招标人和中标人应当自中标通知书发出之日起 7 日内，订立书面合同。

招标人：（章）

招标代理机构：（章）

开封市公共资源交易中心：（章）

2026 年 10 月 8 日