信息化系统运维及云平台服务项目

政府采购合同书

采购人：渭南市精神病医院

供应商：众阳健康科技集团有限公司

签订地点：渭南市精神病医院

项目编号：ZCSP-临渭区-2026-00082　　签订时间：2026年5月26日

采购人：渭南市精神病医院

供应商：众阳健康科技集团有限公司

根据信息化系统运维及云平台服务项目的采购结果，按照《中华人民共和国政府采购法》、《中华人民共和国民法典》等规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

一、合同文件

1、协议书条款；

2、竞争性磋商文件；

3、磋商响应文件；

4、成交通知书；

5、其他。

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

二、合同价款

1、合同总价款为**人民币（大写）：拾柒万捌仟元整（¥：278000.00 元），其中：信息化系统运维：人民币（大写）：壹拾壹万捌仟元整（¥：118000.00 元），云平台服务：人民币（大写）：壹拾陆万元整（¥160000.00 元）。**

2、合同总价款是指完成本次活动包括但不限于本项目的人工费、交通费、管理费、税金、利润及本项目所有风险等一切相关费用，服务期内采购人不再增加任何费用。

3、合同总价一次性包死，不受市场价格变化因素的影响。

三、款项结算

1、合同价款的支付：

合同签订后 7 个工作日内支付 50%的合同价款，半年后支付剩余价款。

2、结算方式：银行转账。

3、支付方式：由采购人负责结算，合同签订后，供应商在接受付款前，开具等额

发票给采购人。

4、供应商银行账户信息

账户名称：众阳健康科技集团有限公司

开户行【 中国工商银行济南自贸区新泺大街支行 】

帐号:【1602160219000270685 】

四、服务地点及服务期

1、服务地点：渭南市精神病医院

2、服务期： 2026 年 05 月 27 日至 2027 年 5 月 26 日（服务期满后，乙方服务合格，同等条件下经双方协商可续约一年）

五、服务内容及要求

（一）服务内容

本项目服务范围涵盖医院信息化系统运维服务及云平台服务，包括但不限于：核心业务系统（HIS、LIS、PACS、EMR、病案系统、门诊叫号系统、门诊电子病历系统、公共卫生上报系统、医保结算清单系统、医院感染实时监控系统等）、基础支撑系统及云平台的日常运维、故障处置、性能优化、安全防护、数据备份与恢复、技术支持等服务。

（二）服务要求

2.1 信息化系统运维服务

2.1.1 软件维护内容

1、维护系统清单

HIS、LIS、PACS、EMR、病案系统、门诊叫号系统、门诊电子病历系统、公共卫生上报系统、医保结算清单系统、医院感染实时监控系统等软件系统。

2、版本升级：

在服务期内升级对已上线使用的信息化软件系统（详见维护系统清单）按需提供当前架构框架内的版本免费升级。

3、日常维护：

对采购人现运行系统客服平台提交的问题进行持续跟踪处理，如新统计查询报表（表单）的制作、现有报表（表单）的修改、用户非正常操作导致的数据修复、调整、客户端工作站疑难问题的排查处理、一般系统故障等，提供实时远程维护，按类别明细如下：

问题类型		响应时间	处理时间
业务运行类		实时沟通及分配	实时电话和微信沟通，一般问题 1 小时内处理，复杂问题 1 小时内提出解决时间及方案。
业务终止类		1 天内分配	优先远程，3 小时内无法恢复立即协调相关人员根据采购人要求以最快的方式到现场
日常客服问题	新增表单、报表类	2 天内分配	10 天内处理完毕，并反馈至信息科
	报表、表单修改类	2 天内分配	5 天内处理完毕，并反馈至信息科
	数据修改提取、对账类	2 天内分配	7 天内处理完毕，并反馈至信息科
	故障排查类（针对软件类）	1 天内分配	5 天内处理完毕，并反馈信息科排查结果

3、流程优化：

根据医院管理需要，结合医院信息管理系统现有功能，协助医院进行内部流程的改造和梳理。

4、性能优化：

提高系统的响应速度和处理能力。

5、系统运维：

根据采购人信息管理系统运行情况，后台检测出不合理流程以及管理缺陷漏洞等，应及时向院方信息化负责人提出，以避免问题的出现导致不可预测的后果。

6、系统监控和维护：

监测系统运行状态、网络流量、磁盘使用情况等，处理系统异常情况，维护系统稳

定性和安全性。

7、故障排除和修复

及时发现并解决系统故障，防止故障扩大和影响范围扩大。

8、数据备份和恢复

对系统数据进行备份，确保数据安全，在系统出现故障时能够快速恢复数据。

9、用户培训和支持

为采购人提供技术支持，解答使用过程中的问题和疑虑，提高采购人对系统的满意度和忠诚度。

2.1.2 接口服务

1、医保接口：

按文件规定或采购人要求完成医保结算业务系统升级等带来的需医保接口开发和升级，不影响医院日常业务。

2、设备接口：

包括院内符合标准传输协议的新设备接口制作及改造，影像类、手术室监护仪设备接口。

备注：不包含所需相关配件费用（如 PACS 采集卡、设备串口连接线等）。

2.2 云平台服务

供应商应具备云平台运维管理和故障排查解决经验，能够解决、修复所使用的软件中的问题。

2.2.1 基础服务要求

1、提供业务系统所需的整体计算能力和业务承载能力保障。

2、云平台可靠性服务：应支持在容错、故障、攻击等场景下，通过冗余、高可用集群、应用与底层设备松耦合等特性来体现，从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性，来实现系统在故障或攻击时服务的正常使用或服务降级时的核心服务，确保服务能力。应能够快速恢复故障应用系统，确保业务的连续性。

3、云平台建设服务：应支持对云平台上业务系统的整体建设，对各个业务系统模块建设资源应支持具体动态调整、网络支持动/静态 BGP 接入、支持 x86 及异构算力等，

保证业务平稳健康运行，并满足业务需求。

应提供计算、存储、网络、安全、容器、数据库、中间件、大数据、人工智能、物联网等多种服务能力，满足当前及未来业务的扩展。

4、平台高可用性服务：应提供云平台业务系统建设过程中所需的中间件支持，应提供稳定的消息队列服务支撑、稳定的高速缓存存储能力支撑、大数据量写入存储能力支持、大数据量日志的数据搜索引擎能力支撑等。

5、云平台服务系统持续集成与持续发布，应支持为整个业务系统敏捷版本发布提供稳定的持续集成与发布能力，提供无故障感知的服务升级能力，提供服务升级灰度发布以及滚动升级能力。

2.2.2 安全服务：

1、应支持为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。VPC 应支持灵活管理云上网络，包括创建子网、设置安全组和网络 ACL、管理路由表、申请弹性公网 IP 和带宽等。通过链路冗余，分布式网关集群，多 AZ 部署等多种技术，保障网络的安全、稳定、高可用性。

2、安全组：应支持为云上虚拟服务器设置合理的安全组管理策略，内网之间仅允许指定业务端口开放。安全组应支持为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，应支持在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

3、Web 应用防火墙（WAF），应支持七层 HTTP 协议的防护策略支持，使用 WEB 应用防火墙或其他防护手段，对常见的 SQL 注入、跨站脚本攻击等进行防御。

应支持对网站业务流量进行全方位检测和防护；应支持对 HTTP(S)请求进行检测，识别并阻断网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定；提供精准高效的威胁检测、针对业界爆发的高危 web 漏洞，应提供快速分析漏洞、向引擎下发漏洞防御规则的支持，保障 0day 漏洞及时在 waf 打上虚拟补丁，用户无感知；应支持通过 Web 应用防火墙服务配置地理位置访问控制规则。可针对指定国家、省份的来源 IP 自定义访问控制；提供简洁友好的控制界面，能实时查看攻击信息和事件日志。

4、企业主机安全，应对云上资源建设主机防护措施，对主机安全行为进行监控，对于恶意注入的木马、病毒等能够扫描并干预。应提升主机整体安全性的服务，提供资产管理、漏洞管理支持检测系统和软件漏洞、Web-CMS 漏洞，识别潜在风险。应支持入侵检测、基线检查等功能，降低主机安全风险；检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性；对运行中的程序进行检测，识别出其中的后门、木马、蠕虫和病毒等恶意程序，帮助用户识别出系统存在的安全风险。

5、云堡垒机，应支持对云上服务器的操作运维审计；提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计；应提供可视化运维行为监控，及时预警发现违规操作；实时记录管理员的资源管理、用户管理和策略管理等所有行为日志，以便监控和审计。

6、数据库安全服务，审计数据库操作行为：应支持对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

7、安全态势感知：应支持统一的威胁检测和风险处置平台；应支持检测出 8 大类的云上安全风险，包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，呈现全局安全攻击态势。

8、云审计：应支持对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等，记录审计日志、审计日志查询、审计日志转储。

9、云监控：应支持一个针对弹性云服务器、带宽等资源的立体化监控平台。资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

10、云日志：应支持日志收集、实时查询、存储等功能，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，提供实时、高效、安全的日志处理能力。

2.2.3、云平台日常运维服务：

1、有专门的运维团队，应支持全时段运维服务，制定科学的管理制度、服务流程、质量管控策略等，形成稳定高效的服务管控体系，做到管理规范、流程合理、职责明确、服务高效。

2、监控服务：云平台基础资源的实时监控与告警，应包括云主机计算资源、内存资源、存储资源等维度的实时监控与分析，对日常业务运行提供业务异常监控，对日常网络带宽提供预警监控，对以上所有监控维度的实时监控与实时告警能力支撑。

3、云平台故障处理服务：根据业务运行需要，应支持对云平台各组件、各项参数进行针对性的调优，如调整资源虚拟化比例、虚拟 CPU 类型与型号、服务线程数量，对业务运行过程中的故障进行分析监测，故障解决，提供 7x24 的检测与处理能力。

4、云平台容量规划与调整服务：应支持对业务需求统计分析，对云平台进行容量规划，包括计算能力、存储容量、网络 IP 地址空间等；实施网络隔离，保障网络安全。

（三）服务质量、标准、期限、效率等要求

1、在服务范围内按工作内容和要求制定详细的方案，方案科学、合理、可靠。

2、人员配备合理。有针对本项目的专项服务小组，项目负责人、工作人员分工明确（应有具体成员名单，包括姓名、工作职责等）

3、有各类突发事件的应急预案和措施，有明确具体的承诺。

4、供应商所拟派的工作人员，若在服务期间发生任何伤害，采购人概不负责，由供应商自行处理。

六、技术资料

1、供应商应按采购文件响应的时间向采购人提供完成项目的有关服务资料。

2、没有采购人事先书面同意，供应商不得将由采购人提供的有关合同或任何合同条文或资料等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。

七、技术情报的保密

1、甲乙双方商定，供应商取得的所有原始技术资料在工作结束后交还采购人，供应商不得对外泄露。

2、相关资料涉及国家秘密的，供应商应严格遵守国家《保密法》及有关保密规定，履行有关保密程序，供应商涉密人员上岗应当经过保密教育培训，掌握保密知识技能，签订保密承诺书，严格遵守保密规章制度，不得泄露国家秘密。

3、运维人员不得以任何方式复制、下载、截屏、导出、外传、分享、传播、售卖、泄露甲方任何数据。

4、严禁私自将甲方数据留存至个人电脑、手机、云盘、U 盘、私人服务器等非甲方指定设备。

5、严禁向任何第三方（含亲友、同行、其他公司、网络社群）透露、讲解、展示甲方数据、系统架构、账号权限及敏感配置。

6、严禁利用运维权限越权查询、篡改、导出、滥用甲方业务数据及用户隐私数据。

7、未经甲方书面正式授权，不得将甲方数据用于本合同约定运维工作**以外**任何用途。

八、转或分包

1、本合同范围的项目服务内容，应由供应商直接服务，不得转让他人；

2、如有转让和未经采购人同意的分包行为，采购人有权解除合同，并追究供应商的违约责任。

九、采购人的权利及义务

（一）采购人的权利

1、采购人有权向供应商询问工作进展情况及相关的内容。

2、采购人有权阐述对具体问题的意见和建议。

3、采购人有权对合同规定范围内供应商的服务行为进行监督和检查，拥有监管权。当采购人认定供应商专业人员不按合同履行其职责，或与第三人串通给采购人造成经济损失的，采购人有权要求更换专业人员，直至终止合同并要求供应商承担相应的赔偿责任。

（二）采购人的义务

1、根据本合同规定，按时向乙方支付应付服务费用。

2、国家法律、法规所规定由甲方承担的其它责任。

十、供应商的权利及义务

（一）供应商的权利

1、根据本合同的约定向采购人收取相关服务费用。

2、供应商在项目实施过程中，有到项目现场勘察的权利。

（二）供应商的义务

1、接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。

2、供应商在履行本合同期间，向采购人提供与本项目有关的一切服务。

3、在服务范围内按工作内容和要求制定详细的方案，建立服务质量标准、保证项目高质量、高标准完成。

4、国家法律、法规所规定由乙方承担的其它责任。

5、项目完成后，供应商应及时向采购人提供成果资料及相关文件。

十一、服务质量标准

达到国家、行业相关规定和现行技术规范、规程合格标准。

十二、知识产权

1、供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如存在前述情形，由供应商承担所有相关责任，并且赔偿由此给采购人带来的损失。采购人享有本项目实施过程中产生的知识成果及知识产权。

2、供应商将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口标准等技术资料，采购人享有使用权。

3、如使用供应商所不拥有的知识产权，则在磋商报价中必须包括合法使用该知识产权的相关费用。

十三、违约责任

（一）采购人因未及时向供应商提供项目启动所需资料、协调地方关系造成服务期延误，每延误1日则本合同服务期延长1日，以此类推；因资料真实性给供应商造成损失和产生相关连带责任时，采购人除按供应商要求进行赔偿外还需承担因连带责任产生的

所有责任。

（二）因供应商原因造成服务期延误（自然灾害等不可抗力除外），采购人有权从未付款项中按每日0.5‰合同价款扣除违约金，此违约以30日为限；若采购人未按约定时间付款，则供应商有权按每日0.5‰合同价款收取违约金。

十四、不可抗力事件处理

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，则合同履行期可延长，其延长期与不可抗力影响期相同。

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。

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。

十五、诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向采购人所在地法院起诉。

十六、合同生效及其它

1、本合同经采购人、供应商法定代表人或其委托人签字并加盖公章后生效。

2、本合同一式陆份，采购人、供应商各执贰份，其余相关部门各壹份。

采购人（章）：

法定代表人

或委托代理人（签字或盖章）：

2016年 5月 26日

供应商（章）：

法定代表人

或委托代理人（签字或盖章）：

2016年 5月 26日