



信息化系统升级服务采购项目

 中国移动通信集团陕西有限公司

合同书

 中国移动通信集团陕西有限公司

 中国移动通信集团陕西有限公司

 中国移动通信集团陕西有限公司

 中国移动通信集团陕西有限公司

 中国移动通信集团陕西有限公司

采购人：渭南市临渭区中医医院

供应商：中国移动通信集团陕西有限公司





签订地点：渭南市临渭区中医医院

项目编号：ZCSP-临渭区-2026-00053

签订时间：2026年4月30日

采购人（甲方）：渭南市临渭区中医医院

供应商（乙方）：中国移动通信集团陕西有限公司

根据信息化系统升级服务采购项目的采购结果，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

(一) 合同价款：人民币（大写）肆拾陆万元（¥460,000.00元），税率6%，不含税金额（大写）肆拾叁万叁仟玖佰陆拾贰元贰角陆分（¥433962.26元）。

(二) 合同总价款是指完成本次服务包含的所有费用，包括本次项目的人工费、验收费、管理费、保险费、磋商文件明示及暗示所有风险等与本项目有关的所有费用，服务期内采购人不再增加任何费用。

(三) 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

(一) 合同价款的支付：合同签订后根据服务进度，按照比例支付服务费，乙方提供相应的税务发票（增值税普通发票）。完成全部项目服务内容并提供相应档案资料，支付服务费的70%，剩余30%服务费于服务验收合格后一次性付清。

(二) 结算方式：银行转账。





(三) 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。

(四) 供应商账户信息：

银行账号：3700024819200005348

开户银行：中国工商银行西安城南科技支行

四、服务期及服务地点

1. 服务期：二年；

2. 服务地点：渭南市临渭区中医医院；

3. 服务内容：详见附件。

五、服务内容及要求

根据信息化系统升级服务采购项目的采购内容，依托中国移动 5G 网络覆盖及云服务能力，提供专线接入、5G 消息、云平台升级、云平台运维服务、云安全服务、云平台日常运维服务等服务工作，提供商详见附件（后附）

六、技术资料

1. 供应商应按磋商文件规定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、规格、计划、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。

七、技术情报的保密

1. 采购人、供应商双方商定，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。

八、转让或分包

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. 采购人有权根据项目的具体情况,要求供应商按期到项目现场勘探解决争议。
4. 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. 采购人应当在约定的时间内,向供应商提供与本项目实施有关的资料。

十、供应商的权利及义务

(一) 供应商的权利

1. 供应商在项目实施过程中,如采购人提供的资料不明确时可向采购人提出书面报告。

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、成交后,供应商向采购人提供项目作业计划和安全责任协议等,其内容包括管理机构的设置、各主要岗位的技术和管理员名单、资质、联系方式及各工种技术工人的安排、项目实施进度安排、技术措施等状况。

- 2、严格按照项目要求进行作业,作业前按项目要求筹备各项器械、材料、工具等,按技术规定进行作业。

- 3、协助采购人及时组织召开检查验收、效果评价和竣工验收工作会议。

- 4、成交供应商向采购人提交施工作业过程性资料和工作总结报告,按相关要求执行。

- 5、有各类突发事件的应急预案和措施,有明确具体的承诺。

十一、验收、结算

1. 质量标准:服务达到国家及行业验收合格标准。

2. 本项目由采购人及相关部门定期对项目进行一次验收。

3. 验收标准:按磋商文件、响应文件及澄清函、项目检查情况等综合指标进行验收。各项指标均应符合验收标准及要求。

4. 甲方应在乙方提交验收申请后7个工作日内进行验收,超过15日仍未组织验收的,视为验收合格。





十二、违约责任

1. 乙方未按合同要求及时提供服务或提供的服务不能满足技术标准和要求，需在甲方指定的期限内无条件重新提供满足甲方需求的相关服务，否则甲方有权解除本合同，甲方解除合同的书面通知书到达乙方之日起合同解除，甲方可不向乙方支付任何费用。

2. 合同生效后，除合同另有约定外，甲、乙双方不得中途毁约，否则视为违约，违约方除向对方支付已发生的各项费用外，还需支付违约金，违约为合同金额的 10%。合同在履行中发生争议，由双方协商解决；协商不成时，任何一方均可向甲方住所地有管辖权的人民法院起诉。

十三、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。

十四、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。

十五、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）：



2026年4月30日

供应商（章）：
法定代表人
或委托代理人（签字或盖章）：



2026年4月30日





附件：

一、基本要求

1. 功能要求：通过采购信息化系统升级服务推动我院信息化建设高质量发展，满足医院需求。

2. 服务期限：一年

3. 服务地点：渭南市临渭区中医医院

二、服务指标的具体要求

1. 服务内容

云升级服务

(1) 要求基于云原生技术，构建高可用服务

需面向医院的业务要求，利用云原生简单易扩展的优势，提供稳定可靠的应用服务。

需利用云原生特性，保障系统在应用快速迭代变化的同时，既可以保持高度的可用性、多节点、负载均衡、弹性扩展等特性，又具备高效处理、水平扩展和数据高并发访问的能力。

(2) 各个业务模块应具有统一的前端框架、设计风格、高度一致的交互体验要求系统从样式、组件、框架、组件交互四个维度实现体验标准化，保障基础体验、交互体验的高度一致。

(3) 采用微服务架构，搭建业务中台、数据中台等中台服务。

要求能够将不同模块、不同业务单元、不同应用程序有机且良好的结合起来，实现服务的轻量化、标准化、快速响应化。

需构建业务中台、数据中台等中台服务，使系统能够提供高可用、高稳定、快速访问和响应的同时，还能够做到服务模块化、可配置化。

(4) 要求将系统，进行云化升级

要求将本地系统迁移到云，实现系统的云化升级。投标人需保证云上的系统与本地系统的衔接和过渡，实现云上系统的正常运行。

(5) 要求使用无版权纠纷的数据库，避免数据制约

为避免因技术问题造成数据库软件不被授权、不能使用，整个医院系统瘫痪等问题；软件升级后需保证数据库无版权纠纷。

(6) 应用+中台架构，支持快速响应政策要求变更

支持在业务中台基础之上，根据国家政策要求变更，复用中台基础能力，快速





构建应用支持。

(7) 要求支持无感升级

应支持在系统升级过程中，无感知、无影响、无侵入；支持灰度发布、金丝雀发布、蓝绿发布、AB发布等常见过渡发布方式。要求业务系统具有完善的预警、监测机制。

(8) 升级模块清单

序号	模块名称	备注
1	HIS 系统	
2	LIS 系统	
3	PACS 系统	
4	EMR 系统 (门诊+住院)	
5	电子病历质量控制系统	
6	门诊叫号系统	
7	病案系统	
8	手术麻醉系统	
9	血液信息管理系统	
10	移动护士端系统	
11	心电网络系统	
12	医院感染管理系统	
13	医院体检信息管理系统	
14	临床路径系统	
15	门诊预约挂号系统	

云运维服务

云运维服务总体要求

云平台运维管理和具备故障排查解决能力。

基础服务：

(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一定的服务能力。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：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撑、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。

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 丰富的功能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。

(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。安全组是一个逻辑上的分组，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；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，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。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；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。

云平台日常运维服务：

(1) 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) 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：应支持根据业务运行需要，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。

服务要求

- (1) 作业能力强，制度健全，管理规范；
- (2) 针对本项目特点，制定科学有效的技术方案和工作方案。

