采购项目编号：HYDZB-2026-053

技术服务合同

政 府 采 购 合 同

采购项目名称：榆林市卫生计生信息中心采购榆林市区域医疗卫生信息化建设运维服务项目包 2

采　购　人：榆林市卫生计生信息中心

成交供应商：西安东软系统集成有限公司

签 署 日 期：2026.9.7

甲方：榆林市卫生计生信息中心

乙方：西安东软系统集成有限公司

甲、乙双方根据 2026 年 08 月 17 日，政府采购编号为 HYDZB-2026-053，招标文件要求和招标结果，并经双方协商一致，达成此合同：

1.项目名称、数量

项目名称	品牌或规格	数量	单价（元）
榆林市卫生计生信息中心采购榆林市区域医疗卫生信息化建设运维服务项目	东软	1	768000.00
合计(大写)	柒拾陆万捌仟元整		

以上项目以人民币进行结算，该价格中包括项目本身价、乙方应缴纳的各种税金、软件原厂维保费用、培训甲方操作人员和交验前的一切费用等。

2. 项目质量要求及乙方对质量负责条件和期限按国家有关规定及相关厂家承诺。

3. 乙方所提交的项目必须符合国家法律法规规定的有关质量安全规定，技术要求见附件一。

4. 交货时间、地点、方式

时间：服务期开始后，乙方开始向甲方提供榆林市卫生计生信息中心榆林市区域医疗卫生信息化软件维保服务。

服务期：2026 年 01 月 01 日至 2026 年 12 月 31 日。

地点：榆林市

方式：现场服务。

5. 付款方式

服务期开始六个月内，乙方提交合法有效全额增值税发票，并经甲方对前半年度运维服务考核合格后，甲方向乙方支付合同总价款的80%（即人民币：614400.00 元，大写：陆拾壹万肆仟肆佰元整）；服务期本年度末，乙方完成全部合同维保义务，提交运维年度总结报告，经甲方年度履约验收合格，甲方向乙方一次性无息付清剩余合同价款（即人民币：153600.00 元，大写：壹拾伍万叁仟陆佰元整）。因财政预算审批、国库支付流程导致付款延后，不属于甲方违约。

6. 违约责任

（1）乙方不能按照规定时间完成系统接口或相关系统的升级改造，每逾期一天乙方需支付给甲方合同总金额 0.1% 的违约金。

（2）当软件出现故障导致系统不能正常访问的，或乙方不能及时配合硬件维保厂家，导致系统崩溃或宕机的，乙方需在 2 小时内排除故障，因系统内部原因导致的，乙方要在 48 小时内解决，因超工作时限导致系统不能正常访问的，每逾期一天，乙方需支付给甲方合同总金额 0.1% 的违约金。

（3）乙方累计支付违约金总额最高不超过本合同总价款的 30%；如违约金不足以弥补甲方实际损失，甲方有权就超出部分另行主张赔偿。

7. 在执行合同期限内，任何一方因不可抗力事件造成不能履行

合同时，应立即通知对方，并寄送有关权威机构出具的证明，则合同履行期可延长，其延长期与不可抗力影响期相同。不可抗力事件延续7 天及以上，双方应通过友好协商，决定是否继续履行合同事宜。

8. 甲乙双方应严格遵守合同约定的权利、义务。

甲方权利、义务：

（1） 组成工作领导小组，负责整个项目的进度管理工作，协调各部门之间的配合，双方的沟通与合作等问题。

（2） 服务期开始后一周内选派、组织掌握计算机知识或熟悉业务的管理人员和技术人员，配合乙方进行合同的实施。

（3） 参与整个项目全过程，协助配合乙方做好需求调研、方案设计及现场等工作，对各项业务的需求报告及时确认，组织相关部门参加各阶段验收工作。

（4） 协调各业务部门配合乙方开展工作，保证乙方及时得到业务相关的技术资料、数据资料，提供业务咨询，并提供现场安装的条件与支持。

（5） 配合乙方的培训工作；必要时在每一处实施现场准备一处能够满足该地软件应用培训需求的专用培训场地，完成包括网络及硬件、系统软件等准备工作，以及投影、打印等相关条件。

（6） 按照工作计划进度，及时接受乙方的验收申请，组织并完成验收工作。

乙方权利、义务：

（7）合同正式生效后指定专门人员成立项目组，该项目组全面

负责整个项目过程，指定现场实施具体负责人，与甲方项目负责人一起全权负责项目管理和协调项目中出现的问题，管理项目进度、需求变更、协调本方资源等多方面的工作。

（8） 要按甲方及相关参数的要求，确定项目组下设的软件开发及实施人员，并在三个工作日内到达现场。项目组的人员变化及时通知甲方，对于不能胜任人员根据本合同要求及时调换。

（9）在甲方配合下根据本合同及附件各项要求完成软件的需求分析、设计、开发、测试和实施工作，及时发现并解决软件问题，不断完善达到软件需求和验收标准的规定；如本服务期内，甲方更换新的系统，乙方需无条件配合甲方及新的系统厂商，完成数据及相关系统的迁移与调试工作。

（10）实施过程由乙方按照 ISO9001：2000 质量体系的要求制定详细规划和工作规范。在甲方配合下制订详细的每周、每阶段的工作计划，明确双方责任和任务，并监督、考核各工作小组的计划执行情况。及时、圆满完成合同约定的内容。

（11）向甲方提供完整的软件相关文档资料。

（12）系统正式运行后，实时监控系统运行状态，当软件出现重大 BUG 及相关问题并影响到甲方实际应用时需及时响应并派人到现场解决。

（13）工作现场严格遵守甲方的规定，完全遵守甲方作息时间，按时上下班，纳入甲方考勤范围，有事要向甲方提出请假申请，并填写请假条，在甲方同意下方可离开工作场所。乙方派驻本项目驻场人

员应当遵守甲方作息及考勤管理制度，履行请假手续。驻场人员未经甲方许可擅自缺勤、旷工，视为乙方服务履约瑕疵，甲方有权从应付本合同服务费中予以扣减，标准为未经许可缺勤每日扣 100 元，旷工每日扣 200 元。乙方自行处理与其派驻员工之间劳动用工关系及劳动报酬。

8-1 转包与分包约定：乙方不得将本项目全部或部分服务转包；如需分包，必须事先取得甲方书面同意，分包不免除乙方全部合同责任。

8-2 履约验收：服务期满开展年度履约验收，验收依据为本合同、附件维保清单、维保达标要求、招标文件；验收由甲方组织，核查运维月报、季度报告、巡检记录、故障处置台账、培训记录、应急预案演练记录等全部运维文档。验收不合格，乙方须限期整改；整改后仍不合格，甲方有权扣减服务费、解除合同并追究乙方违约责任。

9. 因项目或货物的质量问题发生争议时，以甲乙双方共同指定的技术单位的鉴定结果为准。

10. 本合同执行过程中如发生争议，应本着友好的原则协商解决。协商不成产生的诉讼，由属地人民法院管辖。

11. 保障现有软件系统所有功能正常使用，完成政策性调整带来的系统功能改造、监管需求引发的统计报表更新。

12. 软件运维内容

(1) 保障现有软件系统所有功能正常使用，完成政策性调整带来的系统功能改造、监管需求引发的统计报表更新；

(2) 开展平台数据交换、接口联调工作，配合本市已互联互通的卫生机构完成系统调整后的接口联调，保障各级医疗机构、省市平台与区域信息平台的互联互通；

(3) 对软件系统、数据库进行性能测试和效能分析，每月开展 1 次应用软件性能测试，修改优化性能不达标部分；

(4) 保障健康档案、电子病历等核心数据的共享调阅，支撑医疗机构间双向转诊、远程会诊等业务协同功能的正常实现。

13. 本合同未尽事宜，按《中华人民共和国民法典》有关规定签署《补充协议》。

14. 本合同经甲乙双方法定代表人（或委托代理人）签字，并加盖公章（或合同专用章）即为生效。合同一式六份，并在财政局备案，甲乙双方各执两份，财政局一份、采购代理机构一份，效力相同。

15. 本合同共有两份附件，一份为维保内容，另一份为保密协议，合同附件与合同原件享有同等的法律效力。

甲方：榆林市卫生计生信息中心　乙方：西安东软系统集成有限公司

地址：榆林市保宁中路太和巷 3 号　地址：西安市高新区科技二路 68 号西安软件园唐乐阁 C501 室

授权委托代理人（签字）：　　授权委托代理人（签字）：

电话：0912-3838731　　电话：029-86912000

邮政编码：719053　　邮政编码：710065

开户银行：招商银行股份有限公司西安高新技术开发区支行

账号：295081607510001

日期：2026年 9月)日　　日期：26年 9月)日

合同签订地点：榆林市卫生计生信息中心

附件一：

一、维保内容

包 2 软件运维服务清单

序号	软件名称	用途	建设时间
1	标准规范体系	是榆林市医疗卫生数据共享规范与最小数据集标准。 支持区域内各系统和区域医疗卫生信息平台之间的数据级和应用级整合。	2012 年
2	区域医疗卫生数据中心	依托榆林市信息资源中心电子政务外网机房现有软硬件环境，采用服务器托管的模式。建设以健康档案资源库和电子病历索引库为核心的数据库群。	2012 年
3	榆林市区域医疗卫生信息平台	提供云计算管理平台、注册服务、主索引服务、XDS 资源目录服务、适配器、数据转换引擎、动态路由服务、安全隐私服务、主题订阅发布以及集成开发、系统管理、运行监控等功能。	2012 年
4	医疗信息共享与业务协作系统	提供全市居民电子健康档案共享系统。保障患者就诊信息共享、电子病历共享、检查检验共享及调阅服务稳定顺畅；保障医疗机构间双向转诊、远程会诊等医疗协同、业务联动功能高效落地，切实支撑跨机构医疗业务高质量开展。	2012 年
5	区域综合卫生管理系统件	榆林市全民健康信息平台系统。支撑全市范围内医疗服务、公共卫生、医疗保障、卫生资源、计划生育、药品监管等业务的综合监管、统计分析功能。	2012 年
6	基层医疗卫生机构管理信息系统	基层医疗卫生机构管理信息系统，保障基层医疗服务、基本公共卫生、妇幼保健等业务的信息化管理；支撑各级卫生行政管理部门对基层医疗机构的业务监管；包括居民健康监测、健康数据智能分析、健康指导、就医咨询、远程医疗协助和健康信息查询等功能。	2012 年

序号	软件名称	用途	建设时间
7	健康档案浏览器	可集成在各级医疗机构 HIS 系统中，辅助临床医疗，提供历次就诊信息、健康档案、检查检验结果调阅等服务。	2012 年
8	区域医疗卫生信息平台终端用户的接入	终端用户与区域医疗卫生信息平台的互联互通，信息交换共享。	2012 年
9	安全维护	服务器安全维护、软件及操作系统安全维护、网络安全维护、全部硬件安全维护	2012 年

二、维保达标要求

序号	服务名称	主要内容
1	7×24 小时状态监控	对所有基础软件的运行状态进行全天候监控，包括系统进程、资源占用（CPU/内存/磁盘 IO）、数据库连接数、中间件服务状态、虚拟化资源分配等；设置阈值告警机制，异常情况第一时间推送至运维人员并记录告警信息。
2	日常巡检	每周开展 1 次基础软件现场+远程联合巡检，检查系统日志、数据库日志、中间件日志，排查错误指令、异常访问、资源泄漏等问题；每月形成巡检报告，梳理问题隐患并制定整改措施。
3	远程/现场技术支持	提供 7×24 小时远程+现场技术支持，接收到软件使用咨询、故障报修后，远程即时响应解答问题，远程无法解决的故障，运维人员 1 小时内到达现场处置；为业务系统开发、使用人员提供基础软件技术咨询与操作指导。
4	故障诊断与处理	针对基础软件出现的系统宕机、数据库崩溃、中间件服务异常、虚拟化集群故障等问题，按故障级别分级处置；普通故障 4 小时内解决，重大故障 2 小时内解决，特大故障 1 小时内解决；故障处置后进行回测验证，同步完善故障处置档案。
5	性能监测与优化	每季度对基础软件进行一次全面性能检测与分析，针对操作系统资源调度不合理、数据库慢查询、索引失效、中间件连接池配置不当、虚拟化资源分配失衡等问题进行针对性调优；优化后验证性能提升效果，形成性能调优报告。
6	数据备份与恢复	制定基础软件级别的数据备份策略，对数据库全量备份+增量备份结合，每日自动增量备份、每周全量备份，备份文件异地存储；定期开展备份恢复测试，确保故障时能在规定时间内完成数据恢复，保障核心数据不丢失。

序号	服务名称	主要内容
7	补丁与版本管理	跟踪基础软件原厂安全补丁与版本更新信息，结合项目业务运行实际，制定补丁安装方案；在不影响业务系统运行的前提下，完成补丁安装，安装后进行全面测试，确保基础软件与上层业务系统兼容。
8	配置管理	建立基础软件全生命周期配置档案，记录软件版本、安装路径、核心配置参数、数据库表结构、中间件部署信息等；对软件配置的修改、新增进行备案审批，配置变更后进行测试验证，确保不影响上层业务系统运行，同步更新配置档案。
9	安全加固	针对基础软件开展定期安全加固，包括操作系统账户权限管理、数据库访问权限控制、中间件端口防护、关闭无用服务与端口、配置防火墙策略等；每半年开展一次基础软件脆弱性扫描，及时修复安全漏洞，保障基础软件运行安全。
10	日志管理与分析	对基础软件的运行日志、访问日志、故障日志进行统一收集、存储与管理，日志留存时间不低于 1 年；定期对日志进行分析，挖掘异常访问行为、潜在故障隐患，为系统安全与稳定运行提供数据支撑。
11	应急处置与预案管理	制定基础软件突发故障（如系统崩溃、数据损坏、病毒入侵等）专项应急预案，明确处置流程、人员职责、应急措施；每年开展 2 次应急预案实战演练，根据演练结果优化预案内容，提升运维团队应急处置能力。
12	技术培训与文档输出	为项目相关技术人员提供基础软件日常维护、故障排查、性能优化等专项培训，每年至少开展 2 次；按月编制基础软件运维月报，按季度编制性能分析报告，按年度编制运维总结报告，同步整理各类运维文档并归档管理。

附件二：保密协议

保密协议

因乙方参与甲方的信息系统运行维护工作，为确保乙方在工作过程中获取的与甲方信息系统相关的保密信息不被泄露，杜绝网络安全隐患，甲乙双方达成如下协议：

一、保密信息定义

1.维保过程中涉及的技术信息和技术资料，包括但不限于IP地址规划、网络系统架构、软件系统架构、源代码、配置信息、系统登录凭据、系统说明书、维护手册，以及维保过程中的会议文件、备忘、变更、传真、邮件等相关资料；

2.信息系统中存储的所有业务数据；

3.甲方人员及系统用户的电话、邮箱等个人基本信息；

4.在维保过程中经甲乙双方确认的需要保密的其他信息。

二、乙方保密责任

1.乙方应将维保工作中获取的保密信息仅用于维保工作；

2. 乙方在维保工作中获取的保密信息，未经甲方许可，不得提供给第三方；

3.乙方应对维保工作中获取的保密信息进行妥善保管，未经甲方许可不得复制、留存副本；

4.严禁乙方泄露、倒卖保密信息；

5.乙方不得在甲方信息系统所属网络中进行扫描、嗅探，

或通过该网络入侵其他信息系统；

6. 乙方应对其用于存储保密信息的计算机进行安全防护，坚决杜绝保密信息从其计算机中泄露。其计算机应及时安装各类安全补丁程序，并安装杀毒软件，及时升级、定期查杀；

7. 乙方应对其工作人员进行有效管理，并签订保密协议。乙方工作人员在维保项目结束或中途退出维保工作时，应对其持有的保密信息进行销毁；

8. 乙方如发现保密信息被泄露，应及时通知甲方，并积极采取有效措施进行补救。

三、违约责任

因乙方违反本协议造成的保密信息泄露的，乙方应承担相应法律责任，并赔偿甲方损失。

四、其他

本协议作为合同附件，与合同具有同等法律效力。