镇巴县人民医院

供货合同

项目名称：镇巴县人民医院2025年医疗服务与保障能力提升项目合同包3

甲方：镇巴县人民医院

乙方：　汉中网度电子商务有限公司

镇巴县人民医院信息工程购销合同

甲方：镇巴县人民医院　　乙方：**汉中网度电子商务有限公司**

地址：陕西省镇巴县新街 43 号　　地址：陕西省汉中市汉台区前进东路东方之珠小区 6 号楼 604 室

联系人：王金平　　联系人：侯超

联系电话：0916-6716505　　联系电话：13992680796

为明确甲乙双方的责任，确保采购项目的实施，根据《中华人民共和国民法典》规定及招投标文件内容，经甲、乙双方协商同意，签定本合同。

一、设备名称、规格型号、单价、数量

1	2	3	4	5	6	7	8
品目序号	项目名称	生产厂家	规格型号	数量	单价	金额	备注
1	防火墙	深信服科技股份有限公司	AF-1000-L2100	1	89000	89000	
2	同城灾备系统	迪思杰（北京）数据管理技术有限公司	BDMP DC V8.0	1	165000	165000	
3	运维管理系统	超聚变数字技术有限公司	（硬件部分）超聚变 2288H V5	1	129750	129750	
		深圳飞思安诺网络技术有限公司	（软件部分）飞思网巡 IT 运维管理系统 V5.0				
4	安全托管服务	深信服科技股份有限公司	全资产安全托管服务 MSS 套餐	1	102200	102200	
5	攻防演练	北京天融信教育科技有限公司	天融信/攻防演练	1	39500	39500	
6	机房测评	河南泰嵩恒环境监测服务有限公司	泰嵩恒/机房测评	1	33500	33500	
合计金额（大写）： 伍拾伍万捌仟玖佰伍拾元整						￥：558950 元	

二、合同总金额：<u>（金额大写：）　伍拾伍万捌仟玖佰伍拾元</u>

即供应商的所供具体设备内容及其金额。包括所有接口、项目设计、项目工程申报、运输、安装、培训，相关部门验收等费用，其金额不受市场和工作量变化的影响。

三、付款方式

项目计划书按交货时间设计三个阶段实施计划内容，并严格按实施阶段完成项目。乙方人员进场开始施工并向甲方开具合同同等金额的税务发票，支付5%合同款。实施计划第一阶段完成并填写阶段工程进度验收单后，甲方将合同总价的30%汇入乙方账户。实施计划第二阶段完成并填写阶段工程进度验收单后，甲方将合同总价的30%汇入乙方账户。所有项目全部完成，项目运行正常并培训合格后甲方将合同总价的30%汇入乙方账户。留5%余款作为履约金，在质保期满后一次性支付。

四、交货方式

交货时间：合同签订 后45 个日历日

交货地点：甲方指定地点

收货人：徐飞

联系方式：15309162902

交货条件：乙方承担运费及运输保险费。

五、项目验收

乙方在项目实施前应将项目设计方案或图纸提交甲方，获得甲方同意后方可进场实施，项目中如需相关监管单位申报审批，以及项目所有验收需获得政府批复的由乙方全部负责。本项目中所提供系统包括工程类货物应严格按照相关政策标准进行设计和实施并安装到位。

本合同产品出厂前必须做好调试、检验。检验合格后才能发给终端用户。甲方验收合同设备外箱包装有无损坏方可进行开箱验收。乙方保证所供货物的来源渠道正常，产品是全新的（出厂时间必须在合同签订时间前三个月内）、未使用过的；设备的品牌、规格型号、数量与本合同所指明的技术规格及型号相一致；质保期内应对由于产品设计、工艺或材料的缺陷而产生的质量问题负责，否则甲方拒收。双方在安装调试培训验收合格后，在验收单上签字确认。

六、风险责任

项目实施在甲方签字验收前，所有的毁损灭失风险由乙方承担。在甲方签字验收后，其损毁灭失风险由甲方承担。

七、技术保障

1、乙方应随同货物单位提供相应的中文技术文件（包括产品合格证、装箱清单、操作手册、使用说明、检测报告、维护手册、维修手册、服务密码、故障代码表、电路图、服务指南等资料），现场安装、调试、试运行等技术保障服务。

2、乙方免费提供并接入医院和县局现有或者两年内采购的设备、信息系统、

集成平台及县区域平台等系统。

3、投标产品的版本必须为公司现有最新及最高版本。（提供印证资料）

4、与院内其它系统对接后要求高度集成、互联互通，数据统一共享。

5、项目验收应满足三级医院评审、电子病历 5 级，互联互通测试 4 级相关要求.

6、乙方免费提供软件升级：乙方长期免费提供设备的软件升级更换和设备的技术咨询。

7. 投标方所投产品后期可免费升级满足国产信创软硬件及数据库。

8、知识产权：即中标供应商应保证采购人在使用（服务）设备时，不承担任何涉及知识产权的法律风险。

9、招标项目的招标文件、投标文件、补充协议以及合同附件等是本合同不可分割的组成部分，与本合同具有同等法律效力，双方必须遵照执行。

八、技术培训

厂家技术人员对甲方使用维护人员进行操作培训，确保甲方每一位使用人员均能熟练操作，如甲方在使用过程中遇到操作问题，厂家工程师能电话支持，如果需要厂家工程师来院进行再次培训时，乙方应无条件免费到院进行操作培训。

九、售后服务

质保期:经验收合格后，乙方免费保修服务期为 36 个月（其中安全托管服务质保为一年，机房检测和攻防演练为一次性服务）。质保期自甲方在货物验收单（终验）上签字之日起计算。质保期内如遇无法修复的故障，给予免费更换新机。乙方必须在接到甲方通知后 24 小时内响应到达甲方现场维修。保修期后出现故障乙方应继续提供维修技术及配件的供应。在此期间维修仅收原配件成本费，不收取人工费用。

质量保证范围：指并非由于甲方不正当使用而造成的设备故障。

产品的售后服务由“厂家售后工程师”提供。客服电话：

生产厂家	客服电话
深信服（防火墙、安全托管）	400-630-6430
飞思网巡（运维管理系统软件部分）	400-666-8009
超聚变（运维管理系统硬件部分）	400-009-8999
天融信集团（攻防演练）	400-777-0777
泰嵩恒（机房检测）	18611785287/陈
迪士杰（同城灾备系统）	400-600-3889

十、违约责任

乙方因自身原因未按实施计划周表完成工期，或者未全面履行合同义务发生违约，甲方有权终止合同，并向甲方支付合同金额的 3‰的违约金。（按天计算）

甲方因自身原因中途退货，向乙方支付合同金额 3‰的违约金。

十一、不可抗力

1. 合同任何一方由于受诸如洪水、地震等不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，延长的期限应于事故所影响的时间。

2. 遭受不可抗力一方应在不可抗力事故发生后尽快以书面形式通知对方，并于事故发生后14天内将有关部门出具的证明文件、详细情况报告以及不可抗力对履行合同影响程度的说明通知对方。

3. 一旦不可抗力事故的影响持续30天以上，甲乙双方通过友好协商，在合理的时间内达成进一步履行合同或终止合同的协议。

十二、争议的解决

合同执行中发生争议，当事人双方应协商解决，协商达不成一致时，可向甲方当地人民法院提起诉讼。

十三、合同一式五份，甲方三份，乙方一份，政府采购中心一份。

产品配置及备件清单详见附件。

甲　方	乙　方	鉴定方
镇巴县人民医院 （盖章）	（盖章）	
法定代表人：	法定代表人：	
被授权代表：	被授权代表：	
	开户银行：农行汉中汉台支行营业部	
	账号： 26605401040000712	
日期：2025 年 6 月 16 日	日期：2025 年 6 月 16 日	

附件 1　软件功能及配置清单明细：

附件 2　项目实施周期计划表（按投标交货期计算）

附件 1

软件功能及配置清单明细

序号	货物名称	数量	功能及配置详细说明	规格型号	说明
1	防火墙	1	所投产品硬件参数：产品 6 个千兆电口，支持 2 个 USB 口和 1 个 RJ45 串口，冗余电源，1U 机箱；网络层吞吐量 10Gbps，IPS 吞吐量 1Gbps，全威胁吞吐量 800Mbps，并发连接数 400 万，每秒新建连接数 10 万。 所投产品功能参数： 1、所投产品具备国产化 CPU 和国产化操作系统，产品软件为自研，非 OEM 产品，提供三年产品质保和软件升级服务； 2、所投产品具备路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，包括带宽比例、加权流量、线路优先等策略； 3、<u>所投产品具备对 9000 多种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；</u> 4、所投产品具备勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略； 5、所投产品具备服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁 6、所投产品具备 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。	深信服 AF-1000-L2 100	
2	同城灾备系统	1	1、我方提供的“迪思杰数据中心级全数据云灾备管理软件【简称：BDMP DC】V8.0”一整套备份平台，可对 Oracle/SQL 等数据库保护；具备对 Unix/Linux/Windows 等操作系统以及虚拟化平台进行保护。 2、我方提供的“迪思杰数据中心级全数据云灾备管理软件【简称：BDMP DC】V8.0”一整套备份平台硬件指标为：CPU≥24C 2.60GHz *2；内存≥32GB*4；硬盘≥240GB SSD 系统盘*2，16TB*10 块数据盘； 3、我方承诺提供永久授权，容量≥140TB，且不限 license 4、我方提供的产品通过增加系统保护，具备对数据和系统备份，可为被保护的系统提供快速有效的系统	迪思杰 BDMP DC V8.0	

			重建、数据恢复手段。支持 Windows/Linux/AIX/HP-UX 等操作系统，支持 SQL/Qracle/Sybase/DB2 等数据库，支持主流虚拟化平台； 5、产品支持数据库的在线热备功能； 支持数据库的时间点恢复功能，利用数据库的日志将数据库修复到指定的时间点；支持单表直接恢复，要求备份系统在已有的备份数据上能够提供直接的表恢复；支持 Oracle 非归档模式下备份；支持数据库备份的可验证性:备份数据预检测、备份数据模拟预恢复检测、模拟数据库恢复打开验证、结合容灾的自动验证；支持智能合成，可以通过任意一个增量备份版本直接做全量恢复； 6、产品具备完全备份性能：1TB 的数据库全备份时间小于 2 个小时； 恢复性能指标：1TB 的完全恢复时间小于 2 个小时； 单表恢复性能：对于 10g 规模的单表，恢复时间小于 20 分钟； 支持 10 倍源端压缩，避免过多占有网络带宽；具有完善的图形管理控制台，制定相应计划和策略，并提供短信和邮件等监控报警功能。		
3	安全托管服务	1	1、所投服务利用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。 2、所投服务具备互联网暴露面梳理的服务工具，该工具支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息包括域名、域名标题、IP 地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞。 3、所投服务具有云端检测和分析功能，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示。 4、所投服务支持为招标方自定义配置安全规则； 5、所投服务结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。 6、所投服务每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平。 7、本次为招标方配置一名经验丰富的安全管理员，实时响应网络安全相关问题咨询。	深信服全资产安全托管服务 MSS 套餐	

			8、所投服务提供7*24小时的安全守护，不论是白天、黑夜、节假日都应该能做到7*24H在线服务。 9、本次项目安全托管服务资产支持1年的30个服务器、300个PC、院内安全设备服务和安全托管理赔服务。		
4	运维管理系统	1	品牌：超聚变； 外形：标准2U机架式服务器； 处理器：2*Intel Xeon 6226R（2.9GHz/16核）处理器； 内存：64GB DDR4内存，24个DDR4内存插槽，最高2933MT/s，最多12个英特尔®傲腾™持久内存100系列，最高2666MT/s 硬盘：2*480GB SATA SSD，3*2.4T SAS企业级硬盘； RAID：配置SAS/SATA RAID卡，缓存2Gb；可选配支持Cache超级电容保护，提供RAID级别迁移、磁盘漫游、自诊断、Web远程设置等功能； 网络：主板集成2千兆网卡；2个万兆网口(含模块)；1个独立管理端口。 I/O插槽：最多10个PCIe3.0扩展槽位，包括1个RAID卡专用的PCIe扩展卡和1个灵活LOM插卡。 管理：iBMC芯片集成1个专用管理GE网口，提供全面的故障诊断、自动化运维、硬件安全加固等管理特性。 iBMC支持Redfish、SNMP、IPMI2.0等标准接口；提供基于HTML5/VNC KVM的远程管理界面；支持监控、诊断、配置、Agentless及远程控制等带外管理功能，简化管理复杂度；可选配FusionDirector管理软件，提供五大智能等高级管理特性，实现全生命周期智能化、自动化、可视化、精细化管理 电源及外设：配置2*900W白金电源，最大支持2个1500W AC钛金电源；冗余散热风扇，机架安装导轨； 安全特性：支持加电密码、管理员密码、TPM 2.0、安全面板、安全启动、开盖检测等安全特性； 服务：三年免费整机硬件保修，原厂3年质保，原厂7*24小时服务，4小时携配件免费上门服务；	（硬件部分）超聚变2288H V5	
			1、投标产品的系统采用Linux操作系统，内置Linux防火墙模块、MySql数据库。系统为B/S架构，集成IT运维网管和机房动力环境监控以及3D可视化，为一体化产品，统一的人机界面，统一告警通知。系统支持实时监控机房内温湿度、烟雾、漏水、配电、UPS、蓄电池、普通空调、精密空调、门禁、视频监控系统等动力环境设备监控；支持机房链路状态监控；网络设备监控；安全设备监控；服务器硬件状态监控；操作系统监控；支持服务器远程管理；应用服务监控；数据库监控；中间件监控；存储监控。系统标准配置	（软件部分）飞思网巡IT运维管理系统V5.0	

			可监控的 IP 设备许可数量≥200 个。 2、投标产品系统支持国产化统信、麒麟等国产化操作系统，适配东方通中间件，支持龙芯、海光、飞腾等国产化 cpu，可扩展支持国产数据库。 3、系统可扫描自动发现系统所支持的主流品牌网络设备，自动生成图形化展示。必须支持 SNMP V1、V2c、V3 版本。 网络设备应包括 Cisco、华为、H3C、中兴、绿盟、迈普、天融信、锐捷、深信服、F5、Juniper、FortiGate、SecGate、A10 厂家的路由器、交换机、防火墙。系统提供自动网络拓扑发现管理。支持 CDP、STP、FDB、LLDP 多种协议进行扫描，扫描参数可设置发现 IP 区间和屏蔽 IP 区间，设置发现的线程数量以控制发现的速度，自动生成拓扑图，真实反映整个网络状态、链路实时流量情况，设备或链路通过设备图标和链路的颜色变化代表各种监控状态。网络拓扑图管理需支持浏览模式和编辑模式。浏览模式下不能改变设备、链路的位置。 编辑模式下可在视图上进行拖动、添加、删除编辑操作。可实现全屏缩放。提供对齐和布局工具。可对拓扑图进行分组。能提供网络拓扑发现的调试信息下载，能分析整个拓扑发现过程，以确保正确性。 4、系统自动扫描支持 CISCO、HUAWEI、H3C、深信服等品牌的无线 AC、AP,对连接数、在线用户数、上下行吞吐量无线 AC/AP 设备实时数据。 5、系统首页支持自定义视图，可实现用户自行添加网管视图、动环视图， 视图支持全屏显示,支持多屏自动切换，并可自定义切换时间。自定义首页视图默认支持多屏切换。 户无需定制开发与对接数据,根据内置数据源进行自行拖拽即可实现大屏效果。支持网管、动环内置数据元素添加，每个视图最大支持添加 30 个元素。视图支持添加网管、动环的详细数据元素，以数字、文字、图标、进度图、饼图、环形饼图、玫瑰饼图、柱状图、曲线图等方式展示。支持文字、当前时间、多行文字、图片、边框、走马灯、地图等扩展元素。元素支持任意布局，并可按需拖拽、锁定、编辑。		
5	攻防演练	1	本次攻防演练期间，组建专人编制的攻击队，从互联网侧开展攻击，对客户单位的互联网系统及内网进行渗透，以拿到互联网及内网信息系统资产权限或敏感数据为目标，验证客户单位信息系统安全防护能力及应急处置能力；在演练结束后针对发现的问题提出针对性整改建议并出具报告。演练形式为线上+线下。	天融信/攻防演练	

			本次演练将对镇巴县人民医院的关键信息基础设施与重点信息系统目标展开真实攻击与防护的应急演练活动，检验各部门对网络安全事件的发现能力和应急处置能力，积累安全实战应急响应经验，增强安全设施与人才队伍建设，促使安全能力升级，全面提升各部门网络安全意识和关键信息基础设施与重点信息系统网络安全防范能力和水平。 本次演练持续时间 5 天，参演攻击队伍规模为 1 组。 攻击组 由工作组邀请的安全企业攻击人员构成不少于 1 个攻击组，组员需要掌握 WEB 渗透、代码审计、内网渗透等技术。 1. 调研阶段 需求调研主要针对此次攻防演习的背景、组织单位、参与部门、演习目标及演习时间等内容进行明确，并对后续的工作内容进行职责划分。 2. 准备阶段 准备阶段是对攻防演习前期工作的准备，根据本次攻防演习预期达到的目标，梳理出前期需完成的工作，为后续演习正式开展提供保障。 3. 演习阶段 演习阶段作为实战攻防演习的重要阶段，主要包括攻击过程、成果提交等工作。在前期准备工作基础上，对真实网络环境中的系统开展攻击和防守，以力求获取目标系统的最高控制权。 4. 总结阶段 结合本次攻防中挖掘到的漏洞，对本次演习进行全方位的总结。		
6	机房测评	1	对医院新建机房进行环境测评、出具检测报告；具体机房检测项目服务内容如下： 1、电磁辐射系统； 2、洁净度尘埃系统； 3、温湿度系统； 4、噪声系统； 5、照度系统； 6、静电电压系统； 7、正压系统； 8、电源接地系统； 最后出具检测报告。 我方数据中心机房检测公司，在现场检查完成后，整理出系统隐患清单，分析系统运行中的潜在风险及预防措施，分析原设计规划与现有系统高可靠性要求的一致性，分析现行运维管理措施与系统高可靠性要求的一致性。提出对现有基础设施各系统的优化意见和	泰嵩恒/机房测评	

			建议。 如无隐患可直接生成合格检测报告技术文件。如有整改限期整改，整改完成生成合格检测报告技术文件。 9. 评估成果报告交付 泰嵩恒第三方检测评估完成后，泰嵩恒第三方出具合格报告在 7 日内交付委托方，项目完成。		

汉中网度电子商务有限公司

附件2

项目实施周期计划表

序号	实施计划	实施内容	实施周期	备注
1	第一阶段	同城灾备系统完成实施完毕、进入试运行阶段；机房检测完成，出具报告；攻防演练完成，并出具报告；防火墙备货；运维管理系统备货、进行前期准备；安全托管服务进行前期准备。	15个日历日	
2	第二阶段	防火墙交付完成进入试运行；运维管理系统交付完成、进入试运行；安全托管服务前期实施完成进入试运行。	20个日历日	
3	第三阶段	安全托管服务进入常态化服务，所有系统均完全上线进入正式运行并培训完毕，进行移交并提供完整竣工资料。	10个日历日	
4	总计	共计45个日历日完成全部上线工作	合计45个日历日	

汉中网度电子商务有限公司