

第三章 技术、服务及其他要求

（注：本章的技术、服务及其他要求中，带“★”的要求为实质性要求。采购人、代理机构应当根据项目实际要求合理设定，并在第五章符合性审查中明确响应要求。）

3.1. 采购内容

采购包 1:

采购包预算金额（元）：1,782,100.00

采购包最高限价（元）：1,782,100.00

序号	采购品目名称	标的名称	数量 (计量单位)	标的金额 (元)	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及强制采购节能产品	是否涉及优先采购节能产品	是否涉及优先采购环境标志产品
1	C16010500 信息安全软件开发服务	高质量数据集建设安全与密码保护设备和系统	1.00 (项)	1,782,100.00	软件和信息技术服务业	否	否	否	否	否

是否适用本国产品标准：是

报价要求

采购包 1:

序号	报价内容	数量(计量单位)	最高限价	价款形式	报价说明
1	高质量数据集建设安全与密码保护设备和系统	1.00 (项)	1,782,100.00	总价	无

★注：采购包涉及采购货物的，投标人响应产品应当明确品牌和规格型号并指向唯一产品，不能指向唯一产品的，应通过报价表唯一产品说明栏补充说明。

本项目涉及核心产品：

采购包 1:

序号	采购品目名称	标的名称	产品名称
不涉及			

注：涉及核心产品的，具体评审规定见第五章。

本项目涉及采购进口产品：

采购包 1:

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：不涉及采购进口产品时，投标人不得提供进口产品进行响应；涉及采购进口产品时，如国产产品满足采购需求，也可提供国产产品进行响应。

本项目涉及强制采购节能产品：

采购包 1:

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：响应产品属于《节能产品政府采购品目清单》中政府强制采购的产品，投标人应当提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（<http://cx.cnca.cn>）的认证信息截图，否则作无效投标处理。具体要求详见第五章符合性审查表。

本项目涉及优先采购节能产品：

采购包 1:

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《节能产品政府采购品目清单》中优先采购的产品，投标人提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（<http://cx.cnca.cn>）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

本项目涉及优先采购环境标志产品：

采购包 1:

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《环境标志产品政府采购品目清单》中的产品，投标人提供由国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（<http://cx.cnca.cn>）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

3.2. 技术要求

采购包 1:

标的名称：高质量数据集建设安全与密码保护设备和系统

序号	符号标识	技术要求名称	技术参数与性能指标				
1	★	采购清单	序	设备名称	数量	单位	限高单价

			号				(元)
			1	数据库加密与访问系统	3	套	179100
			2	文件加密与访问控制系统	2	套	85000
			3	综合安全网关(千兆)	2	套	60000
			4	VPN 安全网关	12	套	15000
			5	院区外网防火墙	1	台	89000
			6	内网防火墙(安管 区防火墙)	2	台	70000
			7	内网防火墙(服务 器区防火墙)	2	台	124000
			8	院区内网防火墙	2	台	124000
			9	安全隔离与信息 交换系统	1	台	49800
2	★	参数设置	序号	设备名称	参数		备注
			1	数据库加密与访问系统	1、标准 2U 机架式设备，配置冗余电源；采用国产化硬件平台，≥16G DDR4 内存，≥4TB SATA 硬盘；千兆电口数≥4 个，万兆光口≥2 个。 2、支持达梦、人大金仓、瀚高、南大通用等国产数据库。支持 Cache、Mysql、PostgreSQL、Oracle、SQLServer 等常规数据库。 3、支持 SM2/3/4 国密算法，兼容 AES 国际算法。采用二级软件密码模块提供密码运算能力。 4、应用系统免改造，加密后不影响应用的使用。对数据库管理工具、JDBC、ODBC、存储过程、SQL 语句完全透明。加密后不影响数据库的备份、恢复、同步操作。 5、支持表和表空间加密，明文数据不出数据库。不限数据类型，支持所有数据类型。		内网 区

					<p>6、支持应用系统免改造的数据完整性保护。采用 SM3-HMAC 算法对数据进行完整性保护。支持数据库单元格级和行级完整性保护。可以实时感知数据被篡改的行为。可以阻止应用使用被篡改的数据。（提供产品功能截图证明）</p> <p>7、加密后数据库功能零损失，支持精确查询、模糊查询、范围查询、排序查询、联合查询、函数运算、算数运算、数据类型转换。</p> <p>8、支持根据加密粒度分配不同的工作密钥。支持更新、销毁工作密钥，满足密钥轮换需求，提升数据安全性。</p> <p>9、使用硬件密码模块保护顶层密钥。使用三层密钥管理体系对工作密钥逐层保护。明文密钥不出密码模块，保证密钥生命周期安全。</p> <p>10、提供独立于数据库自身权限之外的访问控制体系，支持网关和数据库插件两种访问控制能力，支持双系统鉴别、IP 白名单、字段级访问控制。（提供产品功能截图证明）</p> <p>11、支持 USBKEY、账号口令等多种认证方式。支持多因子认证，具备防绕、防冒能力。</p> <p>12、支持对操作日志进行记录与审计。日志防抵赖，发生安全事件时可准确定位到事故责任人。</p> <p>13、基于门限秘密共享机制备份恢复设备顶层密钥，基于文件机制备份恢复安全策略。支持对备份文件进行机密性与完整性保护。</p> <p>14、支持明密双写，极端情况数据零丢失。产品支持高可用，能够不间断的提供数据加解密服务，保证业务系统的连续性。</p> <p>15、同等条件下，数据库加密后性能损耗小于 10%。</p> <p>16、产品拥有商用密码产品认证证书，满足 GM/T 0028-2024《密码模块安全技术要求》第二级要求。</p> <p>17、产品拥有网络安全专用产品安全检测证书。</p> <p>18、具备《计算机软件著作权登记证书》。</p>	
--	--	--	--	--	---	--

				<p>19、供应商须配合采购人完成不少于 3 套系统商用密码应用安全性评估（密评），承担因所投产品不符合密评要求导致的整改责任。</p>	
				<p>1、CPU：单节点配置 ≥ 20-core ARM、≥ 10 Cortex-X925 + 10 Cortex-A725 ARM。</p> <p>2、内存：单节点配置 ≥ 128 GB LPDDR5x 内存，CPU 与 GPU 共享内存体系，统一系统内存。</p> <p>3、存储：单节点配置：存储容量 ≥ 2TB，支持硬件自加密功能，M.2 NVMe 接口。</p> <p>4、GPU 算力：单节点配置 GPU 卡，GPU 内存带宽 (GB/s) > 270，支持 FP4 稀疏算力 ≥ 1 PFLOP，FP32 峰值性能 ≥ 31 TFLOPS，单机单卡可支持本地部署最大模型参数 ≥ 200B 或 70B 参数模型微调，产品支持双机互联（双卡），双机可支持本地部署最大模型参数 ≥ 405B。</p> <p>5、网络：单节点配置 ≥ 2 个 200G QSFP 端口，支持铜缆连接，1 个 10GbE RJ45 以太网接口，支持 Wi-Fi7，支持蓝牙 5.3。</p> <p>6、支持接口：支持 4 个 USB4 Type C，HDMI 多通道音频输出和 1 $\times$ HDMI 2.1a 显示器接口。</p> <p>7、外形与功耗：支持呼吸灯设置，通过机器底部灯带状态显示机器工作状态。</p> <p>8、产品规格：单节点整机重量 ≤ 1.2kg，支持桌面或边缘部署大模型推理应用，产品尺寸(长 $\times$ 宽 $\times$ 高) ≤ 150mm $\times$ 150mm $\times$ 50.5mm，支持标准办公环境部署。</p> <p>9、安全与可靠性：支持多层安全机制，包括 SROOT、OSROOT、硬件加密引擎、安全启动、内存分区保护，符合 FIPS 140-2 Level 2 与 Modern Device Security Level 1/2/3 合规要求，保障系统与数据安全。</p> <p>10、软件生态：支持各类 AI 模型的快速部署、版本管理和性能优化，支持一键安装和升级，支持双机级联大模型的部</p>	

				<p>署，为 AI 应用提供 Web 应用防火墙，防护恶意攻击和异常访问。</p> <p>11、内置 AI 工具链软件，开箱即用无需授权。自带 AI 应用商店，可部署多种热门 AI 应用，支持应用一键安装和升级；支持面板配置的备份和恢复，确保 AI 应用管理环境安全；支持模型的定时训练、数据同步和模型更新任务；支持系统监控，监控和守护 AI 应用进程，确保服务稳定运行；支持 WAF 防护，为 AI 应用提供 Web 应用防火墙，防护恶意攻击和异常访问。</p>	
		2	文件加密与访问控制系统	<p>1、标准 2U 机架式设备，配置冗余电源；采用国产化硬件平台，≥16G DDR4 内存，≥4TB SATA 硬盘；千兆电口数≥4 个，万兆光口≥2 个。</p> <p>2、对服务器上特定路径或特定类型的文件加密存储。应用系统免改造，加密后不影响应用系统的使用；</p> <p>3、支持基于 SM3 的 HMAC 算法对数据进行完整性保护。</p> <p>4、采用三层密钥保护结构对工作密钥进行逐层保护。使用硬件密码模块保护顶层密钥，支持一文一密。明文密钥不出密码模块，保证密钥生命周期安全；</p> <p>5、支持基于操作系统用户权限的访问控制，只有合法授权的操作系统用户才能访问受保护的文件；支持基于进程的访问控制，只有合法授权的应用才能访问受保护的文件；支持基于时间的访问控制，只有在合法授权访问时间段才能访问受保护的文件。（提供产品功能截图证明）</p> <p>6、至少支持 USBKEY、账号口令认证方式。支持多因子认证，具备防绕、防冒能力。</p> <p>7、详细记录操作日志，支持操作日志的完整性保护。支持操作日志审计，对用户行为和事件进行审计。支持操作行为抗抵赖，可为安全事件定位责任人。</p> <p>8、基于门限秘密共享机制备份恢复设备顶层密钥，基于文件机制备份恢复安全策略。支持对备份文件进行机密性与完</p>	内网区

				<p>完整性保护。（提供产品功能截图证明）</p> <p>9、对文件加密插件进行统一管理，支持插件的上传、下载、删除、启用、禁用、认证、激活功能。</p> <p>10、对应用系统进行统一管理，支持新增、编辑、删除、导入应用进程，实现基于进程的访问控制。</p> <p>11、对透明加密和访问控制等安全策略进行统一管理。</p> <p>12、产品支持主备高可用，能够不间断的提供数据加解密服务，保证业务系统的连续性。</p> <p>13、多文件加解密速率大于 80MB/S。支持百万级加密插件同时在线，并可线性扩展。</p> <p>14、产品拥有商用密码产品认证证书，满足 GM/T 0028-2024《密码模块安全技术要求》第二级要求。</p> <p>15、产品拥有网络安全专用产品安全检测证书。</p> <p>16、具备《计算机软件著作权登记证书》。</p>	
			3	<p>综合安全网关（千兆）</p> <p>1、符合国家密码管理局制定的 GM/T 0022-2014《IPSEC VPN 技术规范》、GM/T 0023-2014《IPSEC VPN 网关产品规范》、GM/T 0024-2014《SSL VPN 技术规范》及 GM/T 0025-2014《SSL VPN 网关产品规范》；</p> <p>2、符合 GM/T 0028-2024《密码模块安全技术要求》密码二级要求；</p> <p>3、采用硬件国产化加密芯片，均具备国家密码管理局颁发的《商用密码产品认证证书》（提供相关证明材料）；</p> <p>4、标准 2U 机架式设备，冗余电源，不小于 6 个千兆电口，不小于 4 个千兆光接口，不小于 2 个万兆光接口；</p> <p>5、IPSec: 大包加密吞吐（1428 字节）：吞吐能力不小于 1.8Gbps；小包加密吞吐（64 字节）：吞吐能力不小于 250Mbps；支持隧道数不小于 5000；SSL 最大并发不小于 30000；SSL 最大新建不小于 400；SSL 加密性能不低于 300Mbps；</p> <p>6、部署模式支持路由模式、透明模式、单臂模式；</p>	

				<p>7、适应 Vlan、Vlan Trunk 环境;</p> <p>8、支持内置 CA, 可为其他设备签发国密双证书;</p> <p>9、支持证书请求的生成, 可由第三方 CA 进行证书签发;</p> <p>10、支持双机热备 (Active-Standby), 支持系统故障自动切换和抢占功能;</p> <p>11、支持管理员分权管理, 不同管理员管理不同的功能模块; 支持管理员的三权分立;</p> <p>12、支持隧道状态查看, 能对关联隧道名称、源/目的保护子网、源/目的隧道地址等进行查看;</p> <p>13、提供基于标准 SSL 的加密通道, 支持应用代理、VPN 隧道多种代理方式, 能有效地支持 IP 层及以上应用协议数据保护;</p> <p>14、客户端支持国产化操作系统: 龙芯平台+UOS 系统、鲲鹏平台+UOS 系统、飞腾平台+UOS 系统、麒麟 990 平台+UOS 系统。</p> <p>15、支持证书、用户名口令、机器码、短信认证因子, 同时支持上述认证因子的组合捆绑认证。</p> <p>16、提供三种工作模式: 标准模式、增强模式、封闭模式(提供相关证明材料)。标准模式: 传统 VPN 客户端, 建立安全虚拟通道; 增强模式: 成功建立安全虚拟通道后, 断开与互联网的连接, 只允许本地终端访问安全网关授权的内网资源; 封闭模式: 客户端在安装到终端设备后, 断开外设接口、禁止其它网络功能。只保留与安全网关通信的能力。在认证成功后, 允许本地终端访问安全网关授权的内网资源。</p>	
			4	<p>VPN 安全网关</p> <p>1、标准 1U 机架式设备, ≥ 6 个千兆电口, ≥ 2 个 2.5GE 口冗余电源, ≥ 10 个 10GE SFP+口, 冗余电源, 内存 $\geq 2G$ DDR3, 硬盘 $\geq 32G$ SSD; 双硬盘支持 Raid0 和 Raid1。</p> <p>2、IPSec 加密速率, 小包 64 字节下加密吞吐性能不低于 20Mbps; 大包 1428 字节下加密性能不低于 250Mbps; IPSec</p>	

				<p>最大并发隧道数≥ 1000条。</p> <p>3、支持 IPsec VPN 智能选路，当有多条可使用的链路能够到达目的网络的情况下，实时地自动探测链路的时延、丢包率，动态切换到满足通信质量要求的链路建立 IPSec 隧道，IPsec VPN 支持 SM1/SM2/SM3/SM4 国密算法。</p> <p>4、支持 DDoS 攻击防御功能，包含 Flood 攻击防御功能、单包攻击防御功能、扫描攻击防御功能、连接速率限制功能。</p> <p>5、SSL VPN 支持多种接入方式，包括 WEB 接入和 IP 接入方式。</p> <p>6、支持 DDoS 攻击防御功能，包含 Flood 攻击防御功能、单包攻击防御功能、扫描攻击防御功能、连接速率限制功能。</p>	
		5	院区外网防火墙	<p>1、网络吞吐量$\geq 18\text{Gbps}$，IPs 吞吐量$\geq 3.5\text{Gbps}$，AV 吞吐量$\geq 3.5\text{Gbps}$，最大并发连接数≥ 400万，最大新建连接数≥ 16万；核心场景指标$\geq$全威胁吞吐量（不含 WAF）$\geq 3\text{Gbps}$，全威胁+WAF 吞吐量$\geq 1.1\text{Gbps}$，IPSec VPN 吞吐量$\geq 1\text{Gbps}$。</p> <p>2、采用国产化芯片和国产化操作系统，硬件质保及软件特征库升级≥ 6年。</p> <p>3、须实现与院内内网态势感知系统（深信服 3.0.98）对接，自动执行联动封锁。</p>	
		6	内网防火墙（安管区防火墙）	<p>1、网络吞吐量$\geq 10\text{Gbps}$，IPs 吞吐量$\geq 2\text{Gbps}$，AV 吞吐量$\geq 2\text{Gbps}$，最大并发连接数≥ 400万，最大新建连接数≥ 10万；核心场景指标$\geq$全威胁吞吐量（不含 WAF）$\geq 1.6\text{Gbps}$，全威胁+WAF 吞吐量$\geq 600\text{Mbps}$，IPSec VPN 吞吐量$\geq 800\text{Mbps}$。</p> <p>2、采用国产化芯片和国产化操作系统，硬件质保及软件特征库升级≥ 6年。</p> <p>3、须实现与院内内网态势感知系统（深信服 3.0.98）对接，自动执行联动封锁。</p>	
		7	内网防火墙（服务器区防	<p>1、网络吞吐量$\geq 45\text{Gbps}$，IPs 吞吐量$\geq 8\text{Gbps}$，AV 吞吐量$\geq 8\text{Gbps}$，最大并发连接数≥ 600万，最大新建连接数≥ 20万；核心场景指标$\geq$全威胁吞吐量（不含 WAF）$\geq 6\text{Gbps}$，全威胁+WAF 吞吐量$\geq 1.2\text{Gbps}$，IPSec VPN 吞吐量$\geq 1.6\text{Gbps}$。</p>	

				<p>火墙)</p> <p>2、采用国产化芯片和国产化操作系统，硬件质保及软件特征库升级≥6年。</p> <p>3、须实现与院内内网态势感知系统(深信服 3.0.98)对接，自动执行联动封锁。</p>	
		8	<p>院区 内网 防火 墙</p>	<p>1、网络吞吐量≥45Gbps，IPs 吞吐量≥8Gbps，AV 吞吐量≥8Gbps，最大并发连接数≥600 万，最大新建连接数≥20 万；核心场景指标≥全威胁吞吐量(不含 WAF)≥6Gbps，全威胁+WAF 吞吐量≥1.2Gbps，IPSec VPN 吞吐量≥1.6Gbps。</p> <p>2、采用国产化芯片和国产化操作系统，硬件质保及软件特征库升级≥6年。</p> <p>3、须实现与院内内网态势感知系统(深信服 3.0.98)对接，自动执行联动封锁。</p>	
		9	<p>安全 隔离 与信 息交 换系 统</p>	<p>1、网络层吞吐≥1Gbps，并发连接数≥10 万，数据库同步性能≥10000 条/秒，1KB 文件同步性能≥3000 个/秒，应用访问延时≤20ms。</p> <p>2、2U 标准机架式设备，采用“2+1”硬件系统架构，单台设备由内、外网两个独立主机模块和一个隔离交换专用硬件模块三部分组成，国产 CPU、操作系统，满足中国信息安全测评中心安全可靠测评名录要求，设备自带 2 块液晶屏、支持蜂鸣告警，实配可插拔冗余电源；内端机：≥8*GE 电口，≥4*GE 光口，≥1 个串口，≥2 个 USB 口，外端机：≥8*GE 电口，≥4*GE 光口，≥1 个串口，≥2 个 USB 口；内外端机各配置≥128GB SSD 硬盘，内外端机各具备 1 个硬盘扩展槽，支持 4T、8T 硬盘扩展；内外端机各具备≥1 个扩展槽，支持电口、光口扩展。</p> <p>3、支持 PostgreSQL、OceanBase、OpenGauss 等同类型数据库之间同步表单信息，配置完成后表单数据同步交换响应正常，数据库清单列表包含 Oracle、MySQL、PostgreSQL、SQL Server、达梦、南大通用、人大金仓、OceanBase、OpenGauss、TIDB、神舟通用、巨杉、GaussDWS、HUAWEI Hive、ODPS、DataHub。</p> <p>4、支持 ftp、Sftp、CIFS/samba、NFS、hdfs、阿里 oss 文件显性和隐性水印，</p>	

					<p>显性水印支持设置水印大小、水印颜色、水印位置，隐性水印无法直接浏览仅通过标签识别，系统支持上传水印文件、输入水印标签的 2 种形式进行水印记录溯源。</p> <p>5、支持对数据库表中的姓名、身份证号码、手机号码、详细地址等敏感数据字段加插数据水印，系统支持上传水印数据库表、输入水印标签的 2 种形式进行水印记录溯源。</p>	
3	★	服务要求	序号	服务类型	服务内容	服务期
			1	基本服务	<p>为保障医院业务高质运行，基本服务至少满足以下内容：</p> <p>1、稳定性：服务期内需保障业务稳定，不无故出现崩溃或宕机现象；</p> <p>2、安全性：具备安全防护机制，做好数据备份，在合同签订后 15 个工作日内提交《安全事件应急响应手册》，重大安全事件（数据泄露、勒索病毒等）30 分钟内电话通报、2 小时内到场、4 小时内出具初步处置报告；</p> <p>3、数据质量：供应商收到异议后，应在 5 个工作日内对数据质量问题进行原因查找和反馈，30 个工作日内对数据质量问题进行数据清洗；</p> <p>4、响应速度：服务期内，采购人通过电话、微信、现场提出的支持需求，供应商须在需求提出的当日完成响应；</p> <p>5、备件供应：服务期内设备故障并经排查，明确 2 小时内无法恢复，应当在 4 小时内提供相同类型和性能的可用机器恢复业务工作，直至故障排除；</p> <p>6、定期巡检：服务期内每月提供至少 1 次软硬件服务期巡检报告；</p> <p>7、培训服务：每年提供 ≥ 2 次培训服务，并在培训前提交培训方案和签</p>	验收合格之日起，提供不低于 6 年

					<p>到表；</p> <p>8、文档服务： 上线运行之日提交本次采购内容的《四川省人民医院应用系统档案》。服务期满后需提交本次采购内容的运维记录签字扫描版本。</p> <p>9、其他：</p> <p>1) 从合同签订生效之日起，采购人每月按照四川省人民医院供应商考核指标对供应商行为进行评价考核，考核结果关联最终付款金额和履约保证金。</p> <p>2) 中标供应商应当与本项目相关的第三方保持有痕的沟通，明确项目的具体要求和功能等方面的细节。采购人负责组织、监督和验收，以确保项目的顺利完成。</p> <p>3) 如涉及因本项目开发的系统原因造成采购人的经济损失，由中标供应商负责向采购人进行赔偿。</p>																																		
			2	质保服务	保证软硬件功能正常运行,提供 7*24 小时质保服务。																																		
4	★	供应商考核	<table><tr><th colspan="5">四川省人民医院供应商考核</th></tr><tr><th>供应 商</th><th colspan="2"></th><th>合同名</th><th colspan="2"></th></tr><tr><th>指标类别</th><th>指标</th><th colspan="3">考核内容</th><th>扣分</th></tr><tr><td rowspan="3">性能 质量 评价</td><td>稳定性</td><td colspan="3">出现故障，导致系统不稳定，影响医院业务：出现故障时间≤30 分钟扣 1 分，30 分钟<出现故障时间且≤60 分钟扣 2 分，>60 分钟扣 5 分；</td><td></td></tr><tr><td>安全性</td><td colspan="3">未具备完善的安全防护机制，存在数据丢失或泄漏的风险，发现一次扣 2 分；采购人有权对现有程序和数据保留备份，供应商违规操作导致采购人机器硬盘中的任何数据和程序损坏或丢失一次扣 5 分； 备份维护不合理，备份数据损坏导致在需要时无法恢复，每次扣 5 分；</td><td></td></tr><tr><td>用户满意度</td><td colspan="3">接到投诉时，一次扣 1 分；出现整改</td><td></td></tr></table>				四川省人民医院供应商考核					供应 商			合同名			指标类别	指标	考核内容			扣分	性能 质量 评价	稳定性	出现故障，导致系统不稳定，影响医院业务：出现故障时间≤30 分钟扣 1 分，30 分钟<出现故障时间且≤60 分钟扣 2 分，>60 分钟扣 5 分；				安全性	未具备完善的安全防护机制，存在数据丢失或泄漏的风险，发现一次扣 2 分；采购人有权对现有程序和数据保留备份，供应商违规操作导致采购人机器硬盘中的任何数据和程序损坏或丢失一次扣 5 分； 备份维护不合理，备份数据损坏导致在需要时无法恢复，每次扣 5 分；				用户满意度	接到投诉时，一次扣 1 分；出现整改			
四川省人民医院供应商考核																																							
供应 商			合同名																																				
指标类别	指标	考核内容			扣分																																		
性能 质量 评价	稳定性	出现故障，导致系统不稳定，影响医院业务：出现故障时间≤30 分钟扣 1 分，30 分钟<出现故障时间且≤60 分钟扣 2 分，>60 分钟扣 5 分；																																					
	安全性	未具备完善的安全防护机制，存在数据丢失或泄漏的风险，发现一次扣 2 分；采购人有权对现有程序和数据保留备份，供应商违规操作导致采购人机器硬盘中的任何数据和程序损坏或丢失一次扣 5 分； 备份维护不合理，备份数据损坏导致在需要时无法恢复，每次扣 5 分；																																					
	用户满意度	接到投诉时，一次扣 1 分；出现整改																																					

					和处理后仍然不满足要求的情况,每5日为一个周期追扣2分,不满一个周期的算一个周期;	
使用支持评价	考勤	驻场工程师每日签到,每次迟到一次扣0.5分;旷工或漏签一次扣1分;				
	响应速度	若需要现场支持时,须及时响应,不响应每次扣1分;发现异常不处理或未向采购人及时汇报,每次扣0.5分;服务期内不接听电话,每次扣0.5分;微信群响应不及时或不按规定响应,每次扣0.1分;				
	备件供应 (本项仅涉及提供硬件的供应商)	不能及时按要求提供所需备件(服务期内设备故障并经排查,明确2小时内无法恢复,应当在4小时内提供相同类型和性能的可用机器恢复业务工作,直至故障排除,超过规定时间无法提供备件一次扣5分;未按规定进行机房基础维护每次扣0.5分;				
	定期巡检	每月定期巡检服务,缺少一次扣1分;没有按要求提供巡检报告的,缺少一次扣1分;				
	培训服务	没有按要求派专业技术人员对医院相关人员进行使用操作、设备维修、保养等技术的培训(不少于2次/年,并提供培训方案和培训签到表),缺少一次扣1分;				
	技术文档	未能在规定时间内按要求提交文档,包括但不限于操作手册、业务数据结构表、运维记录、巡检记录等,缺少一项扣1分;				
	违规违纪评价	廉洁从业	违反行业廉洁要求或违法违纪行为,一旦查实,一票否决			一票否决
	安全规范	不遵守安全生产规范,每次扣2分;				
	其他违规违纪违规	其它不利于医院信息化建设相关行为,视情节严重程度,经采购人讨论酌情扣分				
	扣分合计					

			<div>考核人</div> <div>年 月 日</div>
			<p>备注：</p> <p>1. 服务期内，采购人可按照本项目采购需求内容对应的考核指标对供应商进行考核，具体指标以采购人要求为准；</p> <p>2. 考核关联最终付款金额，具体计算规则如下：</p> <p>1) 平均扣分=服务期汇总考核扣分之总和÷服务期内考核次数；</p> <p>2) 0分<平均扣分≤3分，将对供应商进行诫勉谈话；</p> <p>3) 3分<平均扣分≤5分，对供应商提出警告，从合同待支付金额中或履约保证金中扣除合同总金额 5%费用，扣完为止；</p> <p>4) 5分<平均扣分≤10分，对供应商提出严重警告，从合同待支付金额中或履约保证金中扣除合同总金额 10%费用；</p> <p>5) 10分<平均扣分，视为不合格，终止合同，合同待支付金额和履约保证金（如有履约保证金）不予退还；</p> <p>3. 供应商出现一票否决时，将对其违法违规的相关情况汇报院纪委，同时终止采购合同，扣除所有剩余款项，履约保证金不予退还（如本项目要求缴纳履约保证金），并保留后续追究供应商责任的权利；</p> <p>4. 如合同待支付金额或履约保证金中无款可扣且考核后出现扣款情况，供应商承诺在得到采购人考核结果后的 10 日内向采购人缴纳对应的扣款金额；</p> <p>5. 考核频次为每季度一次；</p> <p>6. 本考核指标最终解释权归四川省医学科学院·四川省人民医院。</p>

3.3. 服务要求

3.3.1. 服务内容要求

采购包 1:

序号	符号标识	服务要求名称	服务要求内容
1	★	付款进度安排 (因系统原因 3.3.2. 商务要求中付款进度安排格式无法修改，因此付款进度安排以此为准。)	合同签订生效且项目验收合格后，供应商向采购人提交请款资料，采购人确认无误后，于 10 个工作日内向供应商支付合同总金额的 100.0% (如有因考核等原因产生的扣款，应在支付前予以扣除)。
2	★	知识产权	由采购人、供应商双方共同开发的项目：采购人、供应商双方共同研发的该系统软件产品，知识产权归采购人、供应商双方共同拥有，软件所有数据归采购人所有。

3.3.2. 商务要求

采购包 1:

序号	符号标识	商务要求名称	商务要求内容
1	★	服务期限	1. 实施时间：本项目合同签订生效后，供应商应在 5 个工作日内开始实施。 2. 实施周期：本项目开始实施之日起 60 日内，完成本项目包含的所有软硬件功能的上线运行。未在实施周期内完成，视为供应商违约，采购人有权终止合同，合同所有款项将不予支付（已缴纳的履约保证金，将不予退还），已支付款项，供应商应于 7 个工作日内退还采购人。
2	★	服务地点	四川省人民医院所有院区。
3	★	验收、交付标准和方法	【注：由于系统固化，若与第二章 2.6.6. 履约验收方案有冲突的，以此处为准】（1）验收组织方式：自行验收。（2）是否邀请本项目的其他供应商：否。（3）是否邀请专家：否。（4）是否邀请服务对象：否。（5）是否邀请第三方检测机构：否。（6）履约验收程序：一次性验收。（7）履约验收时间：供应商完成所有软硬件功能上线运行后 5 日内通知采购人验收，采购人接供应商通知后 10 日内组织验收。（8）验收组织的其他

		<p>事项：验收主体：采购人；验收方式：现场整体验收。（9）履约验收内容：按照基于本项目采购需求编制的采购文件要求及供应商响应文件情况，由供应商向采购人交付的全部软硬件功能。（10）验收标准：①国家相关法律法规、行业标准、技术规范。②基于本项目采购需求编制的采购文件相关技术、服务要求、供应商响应文件相关响应内容。③产品生产厂家出具的产品说明书、技术白皮书等官方技术资料（如涉及）。④如验收时，采购人与供应商认为本项目验收标准中的技术指标、质量要求等内容存在相互抵触或对其理解存在异议，应按照其中更严格的要求、标准等进行验收。⑤按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的要求进行验收。⑥如本项目验收方式为考核验收，则考核结果须为合格。⑦其他标准：无。</p> <p>（11）履约验收其它事项：本项目合同履行过程中，如因国家相关政策法规调整或采购人财政预算发生变动等原因，导致双</p>
--	--	--

			方无法继续履约，采购人有权以书面形式通知供应商，供应商应在收到通知后及时停止履约，并由双方协商解除合同。停止履约后，双方应根据供应商已完成的合格工作量进行费用核算，除经核算的费用外，采购人无需向供应商支付任何其他费用，双方亦互不承担其他违约或赔偿责任。
4	★	支付方式	一次付清
5		付款进度安排	1、/付款条件：（由于系统固化原因无法修改，付款进度安排以 3.3.1. 服务内容要求中的内容为准）。达到该付款条件起 10 个工作日内，支付合同总金额的 100.0%
6	★	违约责任与解决争议的方法	以合同约定为准

3.4. 其他要求

采购包 1:

无