

# 采购清单

| 采购单位   | 西安市胸科医院      |              |            | 备案函号     | ZCBN-西安市-2026-02702 |            |  |
|--------|--------------|--------------|------------|----------|---------------------|------------|--|
| 项目名称   | 内网终端防护系统更新项目 |              |            |          |                     |            |  |
| 政府预算资金 | ¥ 0.00       |              |            | 财政专户管理资金 | ¥ 0.00              |            |  |
| 单位资金   | ¥ 190,000.00 |              |            | 保障性资金    | ¥ 0.00              |            |  |
| 序号     | 品名           | 采购标的         | 单价         | 数量       | 单位                  | 总价         | 技术参数   |
| 1      | 安全集成实施服务     | 内网终端防护系统更新项目 | 190,000.00 | 1        | 项                   | 190,000.00 | <p>1. 本次项目需采购终端安全防御系统与服务器（云主机）安全管理系统，构建“终端统一管控+服务器深度防护+安全态势可视”的一体化安全防护体系，具体目标如下： 1.1业务功能：实现终端杀毒防护、恶意程序查杀、补丁管理、网络准入、合规基线核查；服务器/云主机系统加固、漏洞管理、入侵防御、行为审计、虚拟化防护，覆盖全终端与主机全生命周期安全管理。 1.2核心目标：满足等保2.0三级及医疗行业合规要求，阻断勒索病毒、高级威胁等攻击，杜绝违规外联、数据泄露等风险，保障核心业务7×24小时稳定运行，筑牢终端与主机安全防线。 1.3技术指标：支持B/S架构部署；兼容国产化操作系统（信创/安可适配）；适配医疗设备终端、虚拟化/云环境；支持安全策略统一管控与态势可视化。 1.4经济效益：降低安全事件处置成本与业务中断损失，减少人工运维投入，提升安全管理效率，实现安全投入ROI优化。 2、实施要求 2.1实施范围：本项目所有采购内容，需覆盖采购人同一法人下的所有院区中所有涉及的业务科室。 2.2实施及方案：合同签订后，投标人需现场详细调研，根据调研报告出具包括但不限于施工计划、倒排工期的工作任务分解计划等内容的实施方案。 2.3须全权负责医院现有终端（含医生工作站、护士站、行</p> |

|   |  |  |  |  |  |  |  |
|---|--|--|--|--|--|--|--|
|   |  |  |  |  |  |  | <p>政办公终端、自助机、业务大屏、医疗设备等)及服务器(物理服务器、云服务器)上原有终端安全防护类、网络准入类软件的全面卸载、清理、替换工作,并全程确保不影响医院正常医疗业务开展。</p> <p>2.4确保系统与医院操作系统(含中标麒麟、银河麒麟、Windows等)、业务系统(HIS、LIS、PACS、电子病历等)、数据库及其他安全工具兼容适配,无拦截业务、误报频发等问题,如业务有需要须无条件配合我院进行系统误报、兼容性、拦截等问题排查与解决,确保不影响医院业务系统运行且防护功能正常生效。 2.5根据我院网络架构,须实现无人值守下病毒库的自动更新功能。</p> |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |