韶关市第一人民医院

院内采购文件

项目名称：2026 年度网络安全等级保护测评项目（二次）

项目编号：SYXXK-20260301

采购人：韶关市第一人民医院

二〇二六年四月

目　　录

第一部分　用户需求书

【说明】

1、响应供应商须对本项目的货物或服务进行整体响应，任何只对其中一部分内容进行的响应都被视为无效响应。

2、《采购需求》中凡标注有“★”的地方为实质性响应条款，作为必须响应条款，请响应供应商注意，必须实质性点对点响应；否则将导致无效响应。

3、《采购需求》中凡标注有“▲”的地方为重要条款，但不作为无效响应条款，请响应供应商注意，必须实质性点对点响应；否则将严重影响技术评分。

一、项目概况：

（一）采购方式：院内磋商

（二）采购项目需求一览表：

序号	名称	交付期：	最高限价（元）
1	2026 年度网络安全等级保护测评项目（二次）	2026 年 12 月 30 日前完成所有服务内容并交付所有项目成果。	180,000.00

备注：

1、本项目不接受联合体响应。

2、本次项目包含所有安装、调试、培训、保险费、安装费、检验费、验收费、税金以及培训、质保期服务、各项税费及合同实施过程中应预见和不可预见等完成本采购内容所需的一切费用，采购人不再支付除此之外的其他任何费用。

二、供应商资格

1、响应供应商须提供下列材料（提供资格条件承诺函）：

（1）具有独立承担民事责任能力；

（2）有依法缴纳税收和社会保障资金的良好记录；

（3）具有良好的商业信誉和健全的财务会计制度；

（4）履行合同所必需的设备和专业技术能力；

（5）参加采购活动前三年内，在经营活动中没有重大违法记录。

（6）响应人必须符合法律、行政法规规定的其他条件：单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加本采购项目（或采购包）响应（响应）。

2、信用记录：

供应商未被列入“信用中国”网站（www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网（www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以资格审查人员于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）

3、特定资格：

投标人具有网络安全等级测评与检测评估机构服务认证证书；（须提供有效期内证书复印件，加盖投标人公章）；

三、采购项目技术服务及要求：

测评工具要求

依据 GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》以及 GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》的要求，在等级保护测评过程中，应采用人工访谈、工具检测、登录系统检测、文档分析的方式分析信息系统在等级保护方面与标准要求的差距；然而，为确保成交供应商开展信息系统安全测评的质量以及提高自动化程度，在工具检测方面，成交供应商必须采用符合国家标准的等级保护工具箱及漏洞扫描工具辅助完成测评工作，利用等级保护测评工具箱，提高测评人员工作效率、测评客观公平、测评结果可管理分析汇总。

★为避免产权和使用权纠纷,投标人必须承诺中标后，在签订合同前，提供服务期内使用的软件产品和工具测试样机的自主研发知识产权证明或原厂授权的相关证明文件原件送采购人审查核对，如不能提供测试样机或证明材料原件与投标文件不符，则视为虚假应标，原中标资格废止。采购人有权确认得分排名第二的供应商为中标候选人或重新招标，同时采购人有权向政府采购相关部门投诉，由此引发的所有损失由该投标人承担，**投标文件中提供承诺函并加盖公章，格式自拟**。

1.等级保护检查工具功能要求表

指标项	指标要求
基本功能	工具管理系统应支持八大模块：被检查单位管理、检查计划管理、检查计划执行、检查结果分析、检查知识库管理、检测工具管理、系统管理和退出系统。
离线支撑	应具备离线可作业机制，支持无网络环境脱机作业：
被检单位管理	应包含检查目标单位基本信息、信息系统情况、信息系统定级情况、三级以上信息系统材料、网站安全工作情况和系统资产情况；

	应支持新增、删除、修改被检查单位的信息。
检查计划管理	应包含检查计划名称、被检查单位、检查模板、检查计划时间、被检查的网络系统信息、网络安全责任人信息、检查人员和检查计划附件。
	能支持新增、删除、修改被检查单位的信息，并支持检查计划的导出。
检查计划执行	检查表内容应包括检查范围、检查内容、检查项、检查要点、检查结果、结果记录；可支持生成检查记录单；可支持将检查表单导入平台。
	应支持检查结果录入功能，要求检查结果录入的类型包括选择型、文本型、复合型和复选框型；
	应支持提供检查结果查询功能，针对检查结果状态（例如，是、否、不适用、部分完成）进行查询；
	应支持检测工具检查结果信息的展示功能。
	应支持对检查通知书、检查记录单、处罚决定书、整改通知书、情况通报书、反馈意见和工具检查授权书的编辑、打印和删除。
检查结果分析	支持检查结果信息的展示功能；不同的任务类型应生产不一样的报告；应支持报告汇总导出。
检查知识库管理	应支持对检查模板的新建、删除和编辑；可支持自定义选择模板。
	应内置指标库，应包括网络安全等级保护管理措施重点检查指标、关键信息基础设施安全保护管理重点措施检查指标、网络安全等级保护技术措施重点检查指标、网络安全等级保护技术高风险项检查指标、网络安全等级保护合规检查指标、关键基础设施供应链安全管控能力检查指标、关键信息基础设施运营者供应链安全管理风险检查指标、关键信息基础设施供应链企业网络安全检查指标、网络安全等级保护工作开展情况检查指标、网络安全等级保护专项检查指标；
	应内置知识库，知识库应包括每个指标项对应检查方法、检查对象、判断依据、风险提示
检测工具管理	应支持对检测工具任务进行删除、查看结果和导出结果。
系统管理	应支持为系统运行维护提供支撑，包括配置管理，用户管理，日志管理和系统升级
	应支持对系统版本、工具版本、知识库版本和检查指标库标本的离线升级和在线升级。
资产扫描	▲①支持主机资产列表管理、高级远程管理、监控文件管理、监控数据管理；②通过轻巧的安全探针,快速获取主机的软硬件资产信息；③包括主机资产名称、ip、mac、CPU、内存、硬盘、网卡、操作系统、网络配置、安装软件、账号、服务等内容（中标后需提供以上相关功能模块截图）
口令安全检测工具	工具应默认提供弱口令字典，包括但不限于常见用户名，国内外网络设备默认密码字典、各协议常见默认密码字典；
	支持根据被查单位的人员信息、企业基本信息利用人的密码习惯进行自动化社工分析生成密码字典；
	应支持弱口令扫描功能，支持的弱口令扫描协议不少于 23 种，应包括但不限于 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、WebLogic、Tomcat、SNMP、HTTP 等协议进行弱口令扫描，内置常见弱口令字典；
	应支持导出 word、pdf、XML 等常见格式
新一代漏洞检测工具	应支持针对通用和信创设备进行资产识别，覆盖主流流国产化操作系统、数据库、中间件和其他软硬件；
	支持对通用、信创和开源中间件的漏洞检测，包括但不限于 Windows、Linux、Unix、麒麟、统信 UOS、Openeuler、防火墙、路由器、Log4j2、Struts、Spring 等
	支持对 ORACLE、MySQL、SQL Server、Sybase、PostgreSQL、IRIS 等关系型数据库进行指纹识别和漏洞检测，对 MongoDB、Redis、HBase、Elasticsearch 等非关系型数据库进行指纹识别和漏洞检测
	应支持对 PHP、SSH、FTP、电子邮件等应用系统以及 Office、Apache、WPS 等常用和国产软件进行漏洞检测

		应支持漏洞检出率不小于 90%，误报率应低于 5%；
		应支持多种扫描知识库模板，包括 Windows 扫描、Linux 扫描、大数据相关扫描、摄像头相关扫描、国产系统和软件漏洞扫描、高危漏洞扫描、和全部漏洞扫描，方便用户快速选择
		应支持远程访问方式和授权登录扫描，授权扫描支持 SMB、SSH、RDP、TELNET 等协议
		应支持自动统计总体漏洞数量、操作系统的类型、主机名、开放端口、服务、软件和版本、列出每一个漏洞所存在的主机、漏洞涉及的端口号、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVSS 评分、返回的软件版本信息等
		应支持对数据库进行指纹识别和漏洞检测；设备指纹知识条数不低于 30000 条，其中信创产品指纹不低于 2000 条；
		▲能够支持漏洞验证、历史扫描结果对比和多策略扫描（至少包含主机漏洞扫描、web 漏洞扫描、基于 http 代理的被动 web 扫描、基于日志的被动 web 扫描），且支持扫描的漏洞数量不少于 10 万。（中标后需提供以上相关功能模块截图）
		应支持导出 word、pdf、Excel、XML 等常见格式。
配置检测工具	Windows 主机配置检测工具	▲支持安全扫描，①可发现反动、赌博等内容页面；②检查的目标文件类型支持 PHP、ASP、JSP、ASPX 等脚本类型；③针对检测出来的结果对各类威胁进行自动评分，并按照危险值从高到低进行排序。（中标后需提供以上相关功能模块截图）
		每个检查项应支持给予高、中、低的等级分类，以便于被检查单位优先针对不合规项进行加固修复；
		应支持通过离线脚本的方式直接在目标系统中执行自动化采集相关配置信息和分析，分析结果可导入 Windows 主机配置检查工具进行查看与报告生成。
	Linux 主机配置检测工具	支持对系统进行安全审计检测、恶意代码防范检测、访问控制检测、入侵防范检测、身份鉴别检测、资源控制检测；
		每个检查项支持给予高、中、低的等级分类，以便于被检查单位优先针对不合规项进行加固修复；
		应支持检查目标对象包括国产操作系统和主流操作系统，如中标麒麟、AIX 等；
		支持通过离线脚本的方式直接在目标系统中执行自动化采集相关配置信息和分析，分析结果可导入 Linux 主机配置检查工具进行查看与报告生成。
	网络及安全设备配置检测工具	支持检查是否记录用户登录和操作行为日志、是否开启 NTP 认证功能，确保时钟源可靠；支持检查用户审计记录是否包括时间、用户、事件类型、事件结果（成功/失败）、登录 IP 地址等；支持检查是否配置覆盖每个用户的安全审计功能，对配置策略、修改策略、删除策略、新增用户、修改用户等进行审计
		应支持检查是否配置 NAT 地址转换、是否关闭未使用的网络接口；
		应支持检查是否关闭不必要的服务；
		应支持检查是否修改 SNMP Community 默认通行字、是否使用 SNMPv2 以上版本；
		应支持通过离线脚本的方式直接在网络及安全设备中执行自动化采集相关配置信息和分析，分析结果可导入网络及安全设备配置检测工具进行查看与报告生成，脚本执行应不能对目标系统产生风险
		应支持设备包括 H3C、思科、迪普、华为、天融信、迈普、锐捷、Hillstone、Juniper、奇安信等。
	中间件基线核查检测工具	应支持多种协议类型的远程登录核查，包括 SSH、RDP、TELNET、SMB 等
		应支持的中间件配置检查包括但不限于 Exchange、Bind、Tongweb、Tomcat、WebSphere、Apache、Weblogic、IHS、IIS、Domino、Resin、Jboss、Nginx。
		下载各类离线脚本，离线脚本下载完成之后应可以在检测目标主机上运行对应脚本，并获取结果
		应支持导出 word、pdf、XML 等常见格式
网站安全检测工具		应支持 WEB 2.0，支持各类 JavaScript 脚本解析；
		应支持 JSP、PHP、ASP、.NET 等类型动态页面；

	应支持 IPv4 地址、IPv6 地址、域名地址扫描；
	应支持前后端分离的网站类型扫描；
	应支持易通、DEDECMS、易思、Struts、spring 等框架漏洞扫描；
	应支持对 SQL 注入、Cookies 注入、XSS 跨站脚本、框架注入、伪造跨站点请求、表单绕过、敏感信息泄漏、弱口令、目录遍历、操作系统命令注入、代码执行、文件包含、反序列化漏洞、未授权访问、文件上传、敏感文件、第三方组件、Webshell 后门、其他各类 CGI 等漏洞进行扫描；
	支持基于证书认证的系统扫描（如：网银）
	扫描结果支持提供漏洞参数、HTTP 请求/响应数据，以便用于进行漏洞快速验证或半自动验证漏洞
	应支持导出 word、pdf、Excel、XML 等常见格式
数据库安全检测工具	应支持对数据库“弱点、不安全配置、弱口令、补丁”等方面进行安全检测及准确评估；
	应支持 Oracle、MSSQL、DB2、Informix、MySQL、Sybase、PostgreSQL 等业界主流的数据库；
	应支持达梦、人大金仓、瀚高、优炫、南大通用等国产信创数据库类型；
	应支持远程授权扫描，使用具有 DBA 权限的数据库用户，执行选定的安全策略实现对目标数据库的检测。
主机病毒木马检测工具	应支持快速扫描系统关键目录、快速扫描和发现关键目录中(例如：system32)所存在的病毒与木马程序；
	应支持对系统所有的盘符下的文件进行全面深度检查，帮助发现系统中存在的病毒与木马；
	应支持对选择的目录进行全面的检查，帮助发现指定检查的目录中是否含有病毒程序，支持快速选择桌面、文档、系统关键目录、U 口等区域
	应支持运行在国产操作系统：中标麒麟、银河麒麟、统信 UOS 等
恶意代码检测工具	应支持对指定检查的 WEB 服务器目录路径中的关键文件自动进行网站恶意代码检查，包括 ASP、ASPX、JSP、PHP、CSS 等类型的文件；
	应支持自定义扫描，对指定检查的 WEB 服务器目录路径，自由定制文件类型和检查策略等；
	应支持 IIS、Apache、nginx、weblogic、Websphere、Tomcat 等 WEB 服务器。
固件安全检测工具	应支持 uimage、fit image、zimage、AndroidImage 等多种固件镜像格式；
	应支持固件镜像文件类型识别，包括 Linux 系统固件、小微型系统固件、安卓固件的识别
	应支持解析文件大小、文件哈希、版本信息等固件文件获取固件基本信息；
	应支持配置风险检测，包括但不限于系统弱密码检测、SSH 配置风险检测、FTP 配置风险检测等
	应支持根据固件镜像分析存在的开源组件安全漏洞检测、内核安全漏洞检测；
	应支持离线升级方式
三权分立	网络安全等级保护工具箱的用户分为三类：系统管理员、操作员、审计员
用户登录	采用硬件芯片加密商密算法 KEY 结合登录的形式
工具管理系统	工具管理系统进行加固，应在以下方面应达到网络安全等级保护三级要求：数据安全、密钥管理、痕迹清除、身份鉴别、访问控制、安全审计、通信安全、软件容错、资源控制和恢复出厂设置。

2.漏洞扫描工具功能要求表

指标项	规格要求
总体要求	▲提供自动化渗透测试，测试工具完成自动化渗透测试认定。①支持自动化渗透测试，至少支持探测 SQL 注入、XXE、XSS、任意文件下载、任意文件操作、信息泄露、弱口令、本地文件包含、目录遍历、命令执行等漏洞；②支持部分远程执行、文件

	上传类漏洞自动化利用；③可以自动获取反弹 shell 或者上传 webshell。（中标后要求提供界面截图证明）
	对全网网元进行配置基准安全漏洞检查;
	产品应可灵活调整物理和网络位置，对网络设备进行扫描。扫描结束后生成详细的安全评估报告;
	可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行;
	产品应界面友好，所有的图形界面、报警信息、报表与文档、技术资料要求均需要支持简体中文、英文版本;
安全登录	支持 HTTPS/SSH 安全访问方式;
	支持远程管理，自定义可访问主机网段或 IP;
	支持自定义登陆超时设置，可以在无人操作时自动登出系统;
	支持用户多次登录失败时，自动锁定登录 IP;
扫描策略配置	支持扫描范围自定义、资产导入扫描范围、从文件导入扫描范围;
	支持主机存活探测，支持 ARP、ICMPping、TCPping 及 UDPping 四种类型;
	支持每台主机最大并发线程数设置，至少支持 100 个线程;
	支持每个任务最大并发 IP 数设置，至少支持 10 个并发 IP 扫描检测;
	支持扫描端口范围设置,提供 CONNECT 和 SYN 两种方式对端口进行扫描检测;
	支持通知被扫描主机设置，在扫描主机的时候会向被扫描主机发送 message 消息来通知主机;
	支持显示扫描剩余时间，随时查看扫描进度结果;
	支持多个扫描进度并发统计展示，能够查看历史扫描记录;
	支持多主机、多线程扫描和断点续扫功能;
	支持系统登录扫描，支持 ssh/smb/telnet/pop/pop3/imap/ftp/rsh/rexec/wsus 多种登录方式;
	▲支持系统登录验证功能,对提供的帐号密码进行登陆验证以保证扫描器能正常登陆系统；（中标后要求提供界面截图证明）
	产品要求提供多种缺省扫描策略，并可按照特定的需求，灵活制定目标对象或目标群组，可以同时应用不同扫描策略，并允许自定义扫描策略和扫描参数;
	支持针对已经新建的任务做任务复制，快速生成一个相同任务，支持对复制出来的任务进行再编辑，包括：基本信息、策略、目标范围、调度、扫描参数;
	支持标记任务状态区分出来已修复、误报、新增发现;
	支持单机扫描、分组扫描和全部扫描的设置;
	支持自动定时扫描和多种计划扫描任务管理功能，可按照指定的时间、对象自动扫描，并自动生成报告;
系统漏洞扫描	支持扫描信息应包括主机信息、用户信息、服务信息、漏洞信息等内容。需给出各类扫描信息的详细列表，支持 60000 种以上扫描方法;
	支持对扫描对象安全脆弱性的全面检查，如安全补丁、服务配置等。请详细描述针对主机和网络的扫描类别及项目;
	支持漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、

	CVSS、CNVID、CNNVD、CNCVE、Bugtraq 编号;
	支持可对 Windows 系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris 等目标主机的系统进行扫描;
	支持 SNMP 等协议的漏洞检测;
	支持对国产化操作系统扫描，至少支持麒麟操作系统;
	支持移动设备扫描;
	支持扫描 Cisco、Juniper、华为、F5、Checkpoint 等网络设备;
	支持检测 VMware、KVM 等虚拟化设备;
	支持 Windows 域环境扫描,可针对目标主机的系统配置缺陷及漏洞进行扫描;
数据库漏洞扫描	支持主流数据库漏洞的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2 等;
	支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL 认证，SID、数据库名称、实例名称及实例号等登录选项的设置
	数据库扫描方法为 2500 种以上;
弱密码检测	支持目前知名的检测协议，TELNET、FTP、SSH、POP3、SMB、RDP、Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB;
	支持用户自定义用户名密码列表导入检测;
	支持用户名字典检测、密码字典检测、组合字典检测多种方式;
分布式多级管理	支持引擎或者下级管理中心自动连接上级管理中心;
	支持查看连接状态、拓扑结构、下级引擎状态;
报表能力	报表统计支持漏洞验证，要求提供详细的验证用例，并要求提供详细的测试用例;
	报告应具有易懂的漏洞描述和详尽的安全修补方案建议,并提供相关的技术站点以供管理员参考
	应可根据角色需求产生灵活的报告格式,支持用户自定义报表和预定义报表;
	产品应可灵活定制产生各类报表数据的饼图、柱图等图表信息;
	扫描报告应可对安全的威胁程度分级,并能够形成风险趋势分析报表和主机间风险对比分析报告;
	报表具备导出功能，可以导出不同格式的报表，如 Excel、Word、Html、Pdf、XML 等
	支持动态的显示扫描结果和实时的查看扫描结果;
	支持扫描结果自动发送对比报告至指定邮箱; 发送到指定 FTP 服务器;
	支持扫描完成后进行邮件告警、短信告警、SNMPtrap 告警、SYSLOG 告警、FTP 告警;
	支持扫描结果自动发送短信，支持 http 短信网关;
	支持扫描结果自动发送微信;
资产管理	支持资产自动发现功能，支持利用历史扫描过程中所发现的在线主机信息，来添加部门的资产;
	支持对资产的基本属性、资产价值以及保护等级的属性的修改;
	支持对已有资产的直接扫描;
	支持显示资产的历史扫描结果，支持显示资产的风险评估值; 支持直接查

	看资产的漏洞扫描情况;
	支持对检测漏洞结果进行导出备份;
	支持每个资产历史扫描的风险趋势图显示;
升级、管理	系统应支持自动和人工远程升级以及本地升级。升级内容应包括最新的漏洞库和系统自身的补丁程序;
	支持日志存储告警，能够灵活配置存储空间占用阈值，触发后弹窗告警;
	支持 SSL 的 Web 界面、SSH、Console、Shell 多种方式;
	支持 ping,wget 对网络进行探测;
工具管理加固	工具管理系统进行加固，应在以下方面应达到网络安全等级保护三级要求：数据安全、密钥管理、痕迹清除、身份鉴别、访问控制、安全审计、通信安全、软件容错、资源控制和恢复出厂设置。

四、商务要求

1.对采购人的 4 个网络安全等级保护三级系统进行网络安全等级测评，具体服务需求如下：

序号	需求名称	需求内容
1	等级保护测评	根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）标准要求，对采购人的 4 个网络安全等级保护三级系统进行网络安全等级测评服务： 1、等级保护差距测评 以等级保护标准要求为依据，按照等级保护标准要求对本次项目范围的信息系统进行综合安全评估，发现信息系统的安全保护现状，并为确立安全策略、制定安全规划、开展安全建设提供改进建议，为后续采购人通过网络安全等级保护测评提供指导。等级保护测评的内容至少包括： （1）安全物理环境 安全物理环境测评是对被测系统的机房和办公场所的物理环境安全防护情况进行测评，包括机房物理位置选择、物理访问控制、防盗窃和防破、防雷击、防火、防水和防潮、防静电应、温湿度控制、电力供应、电磁防护等方面的安全状况。 （2）安全通信网络 安全通信网络测评是对被测系统的通信网络安全防护情况进行测评，包括网络架构、通信传输、可信验证等方面的安全状况。 （3）安全区域边界 安全区域边界测评是对被测系统的区域边界的安全防护情况进行测评，包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计、可信验证等方面的安全状况。 （4）安全计算环境 安全计算环境测评是对被测系统的计算环境的安全防护情况进行测评，包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据备份恢复、剩余信息保护、个人信息保护等方面的安全状况。 （5）安全管理中心 安全管理中心测评是对被测系统的管理中心安全保护情况进行测评，包括系统管理、审计管理。 （6）安全管理制度

		安全管理制度测评是对被测系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。 （7）安全管理机构 安全管理机构测评是对被测系统的岗位设置、授权和审批、沟通和合作、审核和检查等情况进行测评。 （8）安全管理人员 安全管理人员测评是对被测系统相关内部人员的人员录用、人员离岗、安全意识教育和培训，以及外部人员访问管理等情况进行测评。 （9）安全建设管理 安全建设管理测评是对被测系统建设过程中的系统定级和备案、安全方案设计、产品采购和使用、自主软件开发、工程实施、测试验收、系统交付、等级保护测评、服务商选择等情况进行测评。 （10）安全运维管理 安全运维管理测评是对被测系统运行维护过程中的环境管理、资产管理、介质管理、设备维护管理、漏洞和风险、网络和系统安全管理、配置管理、恶意代码防范管理、密码管理、变更管理、安全事件处置、应急预案管理等、外包运维管理情况进行测评。 （11）差距测评工作完成后，服务商提交《测评问题清单与整改建议》。 2、安全整改协助服务 协助对机房环境、通信网络、服务器、数据库、中间件、业务系统、源代码、移动应用 APP、办公终端安全实施整改”，改成“协助对机房环境、通信网络、服务器、数据库、中间件、业务系统、源代码、移动应用 APP、办公终端安全问题提供整改咨询 3、等级保护验收测评 在采购人完成此次安全测评的系统风险整改工作后，服务商根据差距测评的结果和风险整改结果进行对比，现场回归测评分析整改结果，对实施的信息系统进行安全等级保护分析及打分，并根据实际测评结论出具符合 2.0 标准的《网络安全等级保护等级测评报告》，并协助采购人通过公安机关的报告审核。
2	渗透测试服务	使用全面渗透方式对采购人 4 个三级系统进行非破坏性的模拟渗透攻击，发现系统可能存在的 SQL 注入、跨站脚本、弱口令、溢出、文件上传、认证会话管理类、未授权访问类等漏洞，并提供针对性整改方案，避免高中危漏洞暴露于互联网，最终出具《渗透测试报告》。
3	小程序安全检测	对四个系统里面的小程序进行安全检测，漏扫和渗透，是否存在缺陷并提出整改建议。
4	网络安全应急演练	根据采购人常面临的网络安全威胁场景，制定相应网络安全应急演练方案，并组织模拟常见网络攻击安全事件进行应急演练，检验采购人网络安全应急响应机制是否存在缺陷并提出整改建议，最终出具《应急演练报告》。
5	服务成果	项目服务成果应包括但不限于以下方面： 1.《网络安全等级保护安全测评报告》； 2.《渗透测试报告》； 3.《应急演练报告》； 4.提供项目实施过程相关过程成果输出物。

五、 服务商认证要求

服务商需严格遵守国家现行的有关标准，公正、独立、自主地开展测评服务工作，需具备以下基础专业认证证书：

1、投标人具有质量管理体系认证证书。（认证范围需明确包含“网络安全等级保护测评”或相关信息技术服务），**或承诺供货时提供有效的质量管理体系认证证书复印件(提供承诺函并加盖公章，格式自拟。)**

六、 服务要求

本项目要求服务商应保证拥有专业信息安全服务人员，保障安全检测工作及时快速响应，服务团队需具有信息安全服务工作经验，应保证项目团队成员的稳定，现场服务人员不得少于**5人**，以保证服务的质量和连贯性。参加过网络安全等级保护测评项目并取得信息安全方面资质证书，服务团队组成架构合理，配备合理的服务团队人员方案，并确保人员的稳定。如更换技术服务人员，需由采购人同意并签字确认。安全服务团队人员应具备以下个人技术能力要求 ：

1、项目经理：

1) 具有公安部第三研究所颁发的网络安全等级测评师（高级）证书；

2、现场技术服务人员（不少于5人）：

1）具有公安部第三研究所颁发的网络安全等级测评师证书；

七、 送货\项目实施要求

1、标准依据

1）《中华人民共和国网络安全法》

2）《中华人民共和国数据安全法》

3）《中华人民共和国个人信息保护法》

4）《关键信息基础设施安全保护条例》（国务院745号令）

5）《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

6）《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

7）《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

8）《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）

9）《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）

10）《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）

11）《信息安全技术网络安全等级保护测评机构能力要求和评估规范》（GB/T 36959-2018）

12）《信息安全技术网络安全等级保护测试评估技术指南》（GB/T 36627-2018）

13）《信息安全技术信息安全风险评估方法》（GB/T 20984-2022）

14）《信息安全技术移动智能终端应用软件安全技术要求和测试评价方法》（GB／T 34975-2017）

15）《移动智能终端软件安全性测试规范》（DB44_T 1557-2015）

16）《信息安全技术代码安全审计规范》（GB/T 39412-2020）

2、服务工具要求

为确保本项目服务质量与效率，服务商应具备较高自动化网络安全服务能力，为确保本项目实施质量，服务商应具备较高自动化服务能力，高质量按时完成等级保护测评、数据安全评估、渗透测试、网络安全应急演练、漏洞扫描等安全服务，确保能客观、快速、准确、全面覆盖本项目的所有需求内容。供应商应在项目实施过程中所使用的工具包括但不仅限以下工具：

（1）具有网络安全等级保护测评及管理工具；

（2）具有网络边界入侵监测追踪工具；

（3）具有网络安全攻防对抗演练平台系统工具

（4）具有数据安全评估工具；

（5）具有网络安全渗透测试工具；

（6）具有源代码安全检测工具；

（7）网络安全漏洞扫描工具；

（8）具有关键信息基础设施安全评估工具。

说明：用于服务本项目的服务工具应由供应商自行提供，服务工具所需的费用已包含在投标总报价内，采购人不再另行支付上述所产生的费用。

3、服务原则要求

（1）客观性和公正性原则：技术服务人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

（2）可重复性和可再现性原则：不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

（3）结果完善性原则：测评所产生的结果应当证明是良好的判断和对测评项的正确理解，测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求 。

（4）最小影响原则：测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），则应做出说明。

（5）规范性原则：信息系统安全等级保护测评服务的实施应由专业的测评服务人员依照规范的操作。

4、服务保密要求

★（1）成交供应商需保证对本项目实施中所获得任何资料和信息严格保密，并与采购人签订保密责任书。（**投标时提交承诺并加盖公章，格式自拟。**）

★（2）本项目范围内的所有技术情报和资料，不向第三方传泄，不论本项目是否变更、解除或终止，本条款均有效。（**投标时提交承诺并加盖公章，格式自拟**。）

★（3）按现行内部规定签订保密约定，项目的资料所有权归采购人所有，成交供应商在任何第三方场合引用相关资料内容都需经采购人同意。（**投标时提交承诺并加盖公章，格式自拟**。）

★（4）在合同期内或合同终止后，未征得采购人书面同意，不向第三方泄露本项目及本合同业务有关的一切资料。否则造成泄密的，成交供应商承担采购人由此引起的损失，若后果严重且触犯法律的，采购人将依法追究其法律责任。（**投标时提交承诺并加盖公章，格式自拟**。）

5、服务现场要求

测评现场除应满足被测设备工作环境外，还应满足以下要求：

（1）网络采取和设定密级相适应的防病毒和安全防护等信息安全措施；

（2）按照设定保密等级要求对现场人员和设备，尤其是可移动存储介质进行管理；

（3）对本次测评有关的测试技术文件、数据等，按照设定密级进行管理。

八、成果清单

项目服务成果应包括但不限于以下方面：

1.《网络安全等级保护安全测评报告》；

2.《渗透测试报告》；

3.《信息系统数据安全评估报告》；

4.《APP 安全检测报告》；

5.提供项目实施过程相关过程成果输出物。

九、安装验收要求

1.验收条件

成交供应商在完成以下服务内容的条件下发起项目验收申请，由采购人组织开展项目验收工作：

（1）完成本项目范围的所有网络安全服务，提交所有项目成果给采购人。

（2）经过采购人同意。

（3）合同或合同附件规定的其他验收条件。

2.验收内容

(1)基础资料：项目有关合同、项目实施方案等。

(2)项目竣工资料：服务成果物、项目其他过程资料及交付物。

3.验收流程

按照合同约定的验收标准完成服务工作，再由成交供应商提出总体验收申请，由采购人组成的专家组对项目进行验收。

十、 交付期

2026 年 12 月 30 日前完成所有服务内容并交付所有项目成果。

十一、 售后服务

（1）成交供应商承诺本项目等级保护测评工作竣工验收通过之日起 1 年内提供 7*8 小时售后咨询服务，所产生的费用包含在投标总报价内，采购人不再另行支付所产生的费用。

（2）为确保本项目的服务质量，成交供应商应具有丰富的同类项目的客户满意度评价案例。

十二、 付款方式

成交供应商为采购人完成上述信息系统验收测评工作并提交《网络安全等级保护测评报告》后并通过验收，向采购人开具合法合规发票，采购方收到发票后 30 个工作日内，采购方向中标方支付合同价款的 100%。

第二部分 评审因素

评审规则：本项目采用综合评分法，经院内专家评审后综合得分最高的推荐为第一成交候选人。

1.评分总值最高为100分，评分分值（权重）分配如下：

评分项目	技术评分	商务评分	价格评分
分值	70	10	20

2.技术评分主要考虑以下因素：

序号	评审内容	分值	评分依据
1	技术参数（标注“▲”部分）响应程度	15	响应供应商提供的产品完全满足用户需求书“第二部分采购需求 采购项目技术服务及要求”中标注“▲”号技术参数条款指标要求的，得15分（一共有5个“▲”）；其中每负偏离或不响应一项扣3分，直至扣完为止。 注：如采购需求中有明确要求提供证明材料的，则以采购需求要求的为准；如采购需求中无明确要求证明材料的，则提供注能够提供上述相关功能截图证明并加盖公章，有缺漏或未提供的本项不得分。
	技术参数（非标注“▲”部分）响应程度	15	对响应供应商所投产品对于用户需求书“第二部分采购需求 **采购项目技术服务及要求**”中非“▲”和非“★”（共计140个)的一般技术要求评审： 1、供应商所投产品技术响应全部满足本项目用户需求书中不带“▲”号、不带“★”号的一般技术要求，得15分； 2、负偏离总数≦5条的，每出现一处负偏离，扣1分，最多扣5分； 3、负偏离总数＞5条的，扣分=5分+[（负偏离总数-5）/（一般技术要求总数-5）]×10，结果四舍五入保留两位小数； 注：采购需求技术要求中未标注“▲”条款中明确要求提供证明资料的，以响应供应商提供的证明资料并加盖响应供应商公章为准，采购需求中没有明确要求提供证明资料的，则以响应供应商提供的“一般技术（服务）参数条款响应表”为证明材料复印件并加盖响应供应商公章。未提供不得分。
3			依照信息系统安全等级保护测评技术标准，在安全技术和安全管理共10个层面进行对标测评；并根据等级测评过程中识别出来的脆弱性问题，结合关联资产的价值和系统面临的威胁情况进行风险分析，识别出较高风险的问

	测评服务方案	14	题，并提出整改建议；综合测评结果汇总及风险分析和评价的结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论。 1.方案内容详细完整、专业，分析要素齐全，方案科学合理可行，完全满足项目需求，得 14 分； 2.方案内容完整、专业，分析要素较齐全，方案较合理，能够满足项目需求，但方案中未包括具体实施细节及措施，得 8 分； 3.方案内容基本完整，分析要素齐全，方案一般，基本满足项目需求，但仅为对招标需求的简单复制，未进行进一步的详细阐述，得 4 分； 4.方案内容及条理性有欠缺，合理性可行性差，无法满足项目需求，得 1 分； 5.未提供不得分。
	质量保证措施	14	为项目制定质量保证方案，对各个阶段的监督检查、评估审计和改进措施进行明确。 1.质量保证措施方案内容完整、详实，有较强的针对性、操作性，得 14 分； 2.质量保证措施方案内容完整，方案较合理，能够满足项目需求，各阶段服务计划完整，得 8 分； 3.质量保证措施方案内容基本完整，分析要素齐全，方案一般，各阶段服务计划完整性有所欠缺，得 4 分； 4.质量保证措施方案欠缺，无法满足项目需求，得 1 分； 5.未提供不得分.
	进度安排控制方案	12	对等保测评服务整个周期的各个阶段进行时间规划和任务明确，包括：等级保护对象分析、安全保护等级确定、定级结果备案、测评准备阶段、方案编制阶段、现场测评阶段和报告编制阶段共七个阶段。 1.项目进度计划安排合理，阶段分明，各阶段人员配备充足，满足项目建设周期、验收要求，得 12 分； 2.项目进度计划安排基本合理，各阶段人员配备满足基本需求，满足项目建设周期、验收要求，得 6 分； 3.项目进度计划安排不合理，各阶段人员配备不足，不满足项目建设周期、验收要求，得 1 分； 4.未提供不得分。

3. 商务评分主要考虑以下因素：

序号	评审内容	分值	评分依据
1	同类业绩	4	投标人自 2023 年 1 月 1 日至今（以合同签订日期为准）完成的等级保护测

			评服务相关业绩，每提供一份合同得 2 分，满分 2 分。 注：须提供合同关键页复印件（合同关键页必须有用户单位名称、合同项目名称、合同标的主要采购内容、签订合同双方的落款盖章、合同签订日期）
2	本项目项目经理资质	6	1、拟派本项目项目经理具备以下能力资质，具有 1 项得 2 分，最高得 2 分： （1）具有网络安全等级测评师证书（高级） 2、项目成员（除项目经理外），同一人员具有多个证书的，可累计计分，最高得 4 分。 （1）具备网络安全等级测评师（中级）证书或以上证书得 2 分；； （2）具备信息（网络）安全等级测评师（初级）证书的得 1 分； （3）具备 CISP 证书的得 1 分； 注：响应文件中同时提供以下证明材料： （1）上述人员名单（格式自拟）； （2）以上证书须提供证书扫描件（或复印件），且提供持证人员开标之日起上推半年内任意连续三个月由投标单位为其缴费的社保证明。

4. **价格评审**

4.1 计算价格评分：

序号	评审内容	评分权重	评分依据
1	价格评审	20	投标报价得分＝（评标基准价/投标报价）×价格分值【注：满足采购文件要求且投标价格最低的投标报价为评标基准价】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。 注：本项目进行线上磋商，若磋商过程无实质性内容改变，则不进行二次报价，以响应文件的报价进行评审。

第三部分　供应商须知

一、费用说明

1、本项目不收取报名费用。

2、本项目不收取履约保证金。

3、本项目不收取投标保证金。

4、本项目不收取招标代理费用。

二、响应文件的数量和签署

1、供应商应编制纸质响应文件（加盖公章）**正本一份和副本两份**，副本可采用正本的复印件。每套响应文件须清楚地标明“正本”、“副本”。若副本与正本不符，以正本为准。

2、响应文件需**双面**打印，并由法定代表人或经其正式授权的代表签字或盖章。授权代表须出具书面授权证明，其《法定代表人授权书》应附在响应文件中。

3、响应文件中的任何重要的插字、涂改和增删，必须由法定代表人或经其正式授权的代表在旁边签字或盖章才有效。

三、响应文件的密封和标记

1、供应商应将响应文件正本和所有的副本密封包装。

2、供应商所提交的响应文件在评审结束后，无论成交与否都不退还。

3、响应文件的有效期为磋商截止日起至少90日历日。

四、合同的订立和履行

1.合同的订立

采购人与成交供应商自成交通知书发出之日起三十日内，按磋商文件要求和成交供应商响应文件承诺签订合同。

2.合同的履行

合同订立后，合同各方不得擅自变更、中止或者终止合同。

五、评审与定标

本项目采用综合评分法，通过资格性、符合性审查的供应商可进入技术、商务评审。以综合评审分数最高者推荐为成交供应商。本项目响应供应商在评审期间需保持电话通畅，评审专家与供应商进行线上磋商，若磋商内容无实质性内容修改，则不进行二次报价，以首轮报价进行价格评审。

磋商小组按照磋商文件确定的评审方法、评审程序和评审标准，对响应文件进行评审，根据综合评分情况，提出书面评审报告，综合得分最高的供应商为第一成交候选供应商，综合得分次高的供应商为第二

成交候选供应商。综合得分相同的情况下，名次由磋商小组讨论决定。

排名第一的中选候选人放弃成交、或因不可抗力提出不能履行合同或拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中选候选人名单排序，确定下一候选人为中选人，也可以重新开展采购活动。

对于首次组织采购时因有效竞标人不足 3 家而重新采购的项目，在二次采购过程中符合要求的供应商只有 1-2 家的，采购活动可以继续进行。二次采购过程中无符合要求的供应商的，发布终止采购活动公告，重新开展采购活动

六、发布中选结果

采购人在评审结束后五个工作日内在韶关市第一人民医院医院官网发布采购结果。成交供应商需自行到新区医院 5 号楼行政楼 207 采购室（0751-8899272）获取成交通知书，不再另行通知。

第四部分 合同书文本

（注：本合同书文本仅供参考，合同签订双方可根据项目的具体要求进行修订。）

韶关市第一人民医院***项目项目合同

合同编号：

甲方： 韶关市第一人民医院

乙方： _____

根据**（项目名称、项目编号）** 的采购结果，按照《中华人民共和国民法典》（合同编）的规定，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、服务内容：详见采购文件 第二部分 用户需求

二、合同金额合同金额为（大写）：人民币____元整（¥___元）。

三、**服务期限：详见采购文件 第二部分 用户需求**

四、服务地点：韶关市第一人民医院，采购人指定地点。

五、甲、乙双方的权力和义务：详见采购文件

六、服务要求：详见采购文件 第二部分 用户需求

七、验收要求：详见采购文件 第二部分 用户需求

八、付款方式：

成交供应商为采购人完成上述信息系统验收测评工作并提交《网络安全等级保护测评报告》后并通过验收，向采购人开具合法合规发票，采购方收到发票后 30 个工作日内，采购方向中标方支付合同价款的 100%。

九、质量检查与奖惩

十、争议的解决

合同执行过程中发生的任何争议，通过友好协商解决。如双方不能通过友好协商解决，任何一方均可向甲方所在地人民法院提起诉讼。

十一、不可抗力

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后 1 日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

十二、税费

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十三、其他

1、本合同所有附件、采购文件、投标（响应）文件、中标（成交）通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2、在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3、如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4、除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

十四、合同生效

1、本合同在甲乙双方法人代表或其授权代表签字盖章后生效。

2、甲、乙双方可对本合同的条款进行补充，以书面形式签订补充协议，补充协议与本合同具有同等效力。

3、合同壹式_____份，甲方执_____份，乙方执_____份。

甲方（采购人）：韶关市第一人民医院　　**乙方（成交人）：**

（公章）

（公章）

甲方代表：　　乙方代表：

签订地点：　　开户名称：

银行账号：

开 户 行：

签订日期：_____年_____月_____日

第五部分　响应文件格式

响 应 文 件

（正本/副本）

项目名称：韶关市第一人民医院***项目

项目编号：　SY

供应商名称：

日期：_____年____月____日

目录

注：

1、请供应商按照以下要求的格式、内容、顺序制作采购响应文件，并请编制目录及页码。否则可能影响对响应文件的评价。

2.供应商所递交的所有资料均应加盖公章。

1、自查表

1.1 资格性自查表

序号	评审内容	自查结论	证明材料
1	**响应供应商须提供以下资料：** （1）具有独立承担民事责任能力：在中华人民共和国境内注册的法人或其他组织或自然人，投标（响应）时提交有效的营业执照（或事业法人登记证或身份证等相关证明）副本复印件。分支机构投标的，须提供总公司和分公司营业执照副本复印件，总公司出具给分支机构的授权书。 （2）有依法缴纳税收和社会保障资金的良好记录：提供《资格条件承诺函》； （3）具有良好的商业信誉和健全的财务会计制度：提供《资格条件承诺函》； （4）履行合同所必需的设备和专业技术能力：提供《资格条件承诺函》； （5）参加政府采购活动前三年内，在经营活动中没有重大违法记录：提供《资格条件承诺函》。重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。（根据财库〔2022〕3号文，“较大数额罚款”认定为200万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于200万元的，从其规定）。 （6）供应商必须符合法律、行政法规规定的其他条件：单位负责人为同一人或者存在直接控股、 管理关系的不同供应商，不得同时参加本采购项目（或采购包） 投标（响应）。 2、信用记录： 供应商未被列入“信用中国”网站（www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网（www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以资格审查人员于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网	□通过 □不通过	见响应文件第___页

	（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）。（提供**信用记录自查承诺函）** 3、特定资格： 投标人具有网络安全等级测评与检测评估机构服务认证证书；（须提供有效期内证书复印件，加盖投标人公章）；		

备注：以上材料将作为响应供应商有效性审核的重要内容之一，响应供应商必须严格按照其内容及序列要求在响应文件中对应如实提供，对资格性证明文件的任何缺漏和不符合项将会直接导致无效响应！本表不得自行删减！请在对应的□打“√”。

1.2 符合性自查表

序号	评审内容	自查结论	证明材料
1	投标报价不高于采购需求规定的最高限价/采购预算金额	□通过 □不通过	见响应文件 第_____页
2	已提交响应函，且响应有效期不少于磋商文件中载明的响应有效期；	□通过 □不通过	见响应文件 第_____页
3	已按磋商文件要求提供法定代表人/负责人证明书（附法定代表人/负责人身份证复印件）及授权委托书（附被授权人身份证复印件）的。	□通过 □不通过	见响应文件 第_____页
4	响应文件完全满足磋商文件的实质性条款（即标注★号条款） 无负偏离的；	□通过 □不通过	见响应文件 第_____页

备注：

以上材料将作为响应供应商有效性审核的重要内容之一，响应供应商必须严格按照其内容及序列要求在响应文件中对应如实提供，对符合性证明文件的任何缺漏和不符合项将会直接导致无效响应！请在对应的□打“√”。

2、响应函（以下内容只可增加，不可删减）

响应函

致：**韶关市第一人民医院**

我方愿参与响应你方组织的_____（项目名称）_____的磋商活动[项目编号为：_____]。我方确认收到贵方提供的_____（项目名称）_____的磋商文件的全部内容。

我方在参与响应前已详细研究了磋商文件的所有内容，包括澄清、修改文件（如果有）和所有已提供的参考资料以及有关附件，我方完全明白并认为此磋商文件没有倾向性，也不存在排斥潜在响应供应商的内容，我方同意磋商文件的相关条款，放弃对磋商文件提出误解和质疑的一切权力。

*(响应供应商名称)*作为响应供应商正式授权*(授权代表全名,职务)*代表我方全权处理有关本磋商的一切事宜。

在此提交的响应文件，纸质文件（加盖公章）正本一份，副本二份；

我方已完全明白磋商文件的所有条款要求，并承诺如下：

（一）**本响应文件的有效期为响应截止时间起 90 天。**如中选，有效期将延至合同终止日为止。在此提交的资格证明文件如有在响应有效期内失效的，我方承诺在成交后补齐一切手续，保证所有资格证明文件能在签订磋商合同时直至磋商合同终止日有效。

（二）我方同意按照贵方可能提出的要求而提供与磋商有关的任何其它数据、信息或资料。

（三）我方如果成交，将保证履行磋商文件及其澄清、修改文件（如果有）中的全部责任和义务，按质、按量、按期完成《用户需求》及《合同书》中的全部任务。

（四）我方承诺对全部磋商内容进行响应。

（五）在本次采购过程中，我方独立参与响应，并未与其他公司或组织组成联合体。我方承诺不转包、分包。

（五）我方承诺响应文件内容符合国家法律法规的相关规定，无法定或磋商文件规定的无效响应的其他情形。

（六）我方承诺响应文件未含有贵院不能接受的附加条件。

（七）我方对在本函及响应文件中所作的所有承诺承担法律责任。

（八）我方完全响应商务条款要求的所有要求的内容，设备整机原厂保修_____年。

（九）本公司（企业）承诺在本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

（十）我方已充分了解本项目的实际工作要求和质量要求，结合自身能力因素及市场价格变动趋势充分考虑，并愿意承担由此带来的风险，保证中选后能提供满足磋商人所需的要求。所有项目定价后在合同履行期间不因市场价格、人力成本上涨等因素或其他理由暂停或终止服务。

（十一）若我方中选，在合同签订前，向采购人提供本项目医疗器械产品注册时的检测报告进行验证，

若检测报告中的参数不符合本项目的参数要求，采购人将有权取消我公司（企业）的成交资格，并有权确定下一候选人为成交供应商或重新开展采购活动。造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

（十二）所有与磋商有关的函件请发往下列地址：

地　　址：_____ 邮政编码：_____

电　　话：_____

传　　真：_____

代表姓名：_____ 职　　务：_____

响应供应商法定代表人/负责人（或法定代表人/负责人授权代表）签字或盖私章：_____

响应供应商名称（盖章）：_____

日期：_____年_____月____日

3 资格证明文件

3.1 资格条件承诺函

资格条件承诺函

我方 （响应人名称） 符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（三）项、第（四）项、第（五）项规定条件，具体包括：

1.具有良好的商业信誉和健全的财务会计制度；

2.具有履行合同所必需的设备和专业技术能力；

3.具有依法缴纳税收和社会保障资金的良好记录；

4.参加本次磋商活动前三年内，在经营活动中没有重大违法记录；

5.符合法律、行政法规规定的其他条件；

6.我方与其他响应人不存在单位负责人为同一人或者存在直接控股、管理关系；

7.我方承诺未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务；

我方对上述承诺的真实性负责，在评审环节结束后，自愿接受采购单位的检查核验，配合提供相关证明

材料，证明符合《中华人民共和国政府采购法》规定的响应人基本资格条件。如有虚假，将依法承担相应法律责任。

特此承诺。

供应商名称（公章）

年　月　日

供应商名称（公章）

年　月　日

3.2 信用记录自查承诺函

信用记录自查承诺函

韶关市第一人民医院：

关于本企业信用情况，经对“信用中国”网站（www.creditchina.gov.cn）中企业信用信息、“国家企业信用信息公示系统”（http://www.gsxt.gov.cn/corp-query-homepage.html）信息查询、“政府采购网”（ www.ccgp.gov.cn）政府采购严重违法失信行为等查询结果，截至规定的报价响应截止时间，我司没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合规定条件的供应商名单中。特此承诺！

供应商法定代表人（或法定代表人授权代表）签字：_____

供应商名称（加盖公章）：_____

日期：_____年_____ 月____ 日

备注：采购人将对供应商承诺内容的真实性和有效性进行审查、验证，如有造假或情况不一致，将导致响应无效！

3.3　公司有效的《营业执照》复印件或多证合一证件的复印件

3.4　法定代表人/负责人证明书

法定代表人/负责人资格证明书

韶关市第一人民医院：

_____同志，现任我公司_____职务，为法定代表人，特此证明。

法定代表人签字（盖章）：_____　　法人联系电话（手机）：_____

公司名称（单位公章）：_____

公司主营：_____

公司兼营：_____

签发日期：_____

说明：1.法定代表人为企业事业单位、国家机关、社会团体的主要行政负责人。

2.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

3.此证明书将作为合同不可分割的组成部分。

此处粘贴法定代表人 身份证正面	此处粘贴法定代表人 身份证反面

3.5　　法定代表人/负责人授权委托书（如有）

法定代表人/负责人授权委托书

韶关市第一人民医院：

兹授权_____同志，为我方签订经济合同及办理其他事务代理人，其权限是：全权代表本公司参与_____（项目名称）_____的报价响应，负责提供与签署确认一切文书资料，以及向贵方递交的任何补充承诺等。

授权公司（单位盖章）：_____

法定代表人（签字或盖章）：_____

授权代理人（签字或盖章）：_____　职务：_____　联系电话（手机）：_____

有效期限：至 _____年 ____ 月 ___日　　签发日期：_____

说明：1.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

2.此证明书将作为合同不可分割的组成部分。

3.供应商签字代表为法定代表人，则本表不适用。

此处粘贴授权代理人 身份证正面	此处粘贴授权代理人 身份证反面

3.6、企业股东构成情况表

企业股东构成情况表

企业名称			
注册地址		企业类型	
法定代表人姓名		电话	

股东及出资信息						
序号	股东名称（姓名/股东全称）	股东类型（自然人股东/法人股东）	身份证号/统一社会信用代码	出资额（万元）	出资方式	占全部股份比例

备注：

1.股东或出资人为自然人的，填写自然人姓名及身份证号；股东或出资人为法人的，填写法人企业全称及统一社会信用代码。出资方式填写：货物、实物、工艺产权和非专利技术、土地使用权等。2.响应供应商必须如实填写股东构成情况，具体信息情况应与“国家企业信用信息公示系统”（网站：http://gsxt.gdgs.gov.cn/）查询的信息一致。

4、参数响应表

4.1、实质性响应一览表（用户需求中带“★”号条款，集中统一罗列，若有）

序号	采购要求 实质性条款（“★”号条款）	实际投标/响应情况	是否偏离（无偏离/正偏离/负偏离）	证明文件（如有）
1				见响应文件（）页
2				见响应文件（）页
3				见响应文件（）页

4				见响应文件（）页
5				见响应文件（）页
6				见响应文件（）页

注：

1.供应商必须对应采购文件所有实质性条款（“★”号条款）内容进行逐条响应，如有缺漏，缺漏项视同不符合负偏离。如采购文件无“★”号条款要求，则在此表空白处填写“采购文件无“★”号条款要求”。

2.供应商响应采购需求应具体、明确，含糊不清、不确切或伪造、变造证明材料的，按照不完全响应或者完全不响应处理。构成提供虚假材料的，移送监管部门查处。

3.本表内容不得擅自修改。

供应商法定代表人（或法定代表人授权代表）签字或盖章：_____

供应商名称（盖章）：_____

日期：　　年　　月　　日

4.2、重要参数条款响应表（第二部分采购需求 采购项目技术服务及要求中带“▲”号条款，集中统一罗列）

项目名称：XXXXX

项目编号：XXXXX

序号	采购需求带“▲”号条款内容	是否响应	偏离说明	响应页码
1				
2				
3				
…				

说明：1.供应商必须对应采购文件的 “▲”号条款逐条应答并按要求填写下表。

2.对完全响应的条目在下表相应列中标注“是”。对有偏离的条目在下表相应列中标注“否”，并简述偏离内容。

3、采购文件中如没有“▲”号条款，此表格不用填写。

供应商名称（加盖公章）：

法定代表人（或授权代表）签字：

日期：　　年　　月　　日

4.3 一般技术（服务）条款响应表（第二部分采购需求 采购项目技术服务及要求”中非“▲”和非“★”，统一集中罗列）

项目名称：XXXXX

项目编号：XXXXX

序号	采购需求一般技术（服务）参数条款内容	是否响应	偏离说明	响应页码
1				
2				
3				
…				

说明：1.供应商必须对应采购文件的**非“▲”、非“★”**号条款逐条应答并按要求填写下表。

2.对完全响应的条目在下表相应列中标注“是”。对有偏离的条目在下表相应列中标注“否”，并简述偏离内容。

3、采购文件中如没有**非“▲”、非“★”**号条款，此表格不用填写。

供应商名称（加盖公章）：

法定代表人（或授权代表）签字：

日期：　年　月　日

4.4 商务条款响应表

1、商务条款响应表

[说明]供应商应对照磋商文件第二部分《采购需求》所列商务条款的内容一一响应，完全满足的在“是否响应”栏中填写“完全响应”，不能满足的填写“否”，有差异的则在“差异内容”栏中写明差异内容。

序号	采购文件商务要求		响应文件内容		响应页码（如有）
	条目	简要内容	是否响应	差异内容	

供应商名称（加盖公章）：

法定代表人（或授权代表）签字：

日期：　　年　　月　　日

4.5 同类项目业绩表（如有）

项目名称：XXXXX

项目编号：XXXXX

序号	业主名称	项目名称	合同总价	签约日期	业主单位 联系人及电话
1					
2					
…					
小计					

注：供应商应提供合同复印件关键页等相关证明附件，具体按商务评审表要求提供。

供应商名称（加盖公章）：

法定代表人（或授权代表）签字：

日期：　　年　　月　　日

五、评审自查表

5.1 商务评审自查表

序号	评审内容	评分准则	证明文件
1			见响应件第_____页
2			见响应件第_____页
3			见响应件第_____页
….			见响应件第_____页
说明：供应商结合磋商文件中商务部分评审内容，并注明每项评审内容对应的响应文件所在页码，以便查对。			

5.2 技术评审自查表

序号	评审内容	评分准则	证明文件
1			见响应件第_____页
2			见响应件第_____页
3			见响应件第_____页
….			见响应件第_____

			页
说明：供应商结合磋商文件中技术部分评审内容，并注明每项评审内容对应的响应文件所在页码，以便查对。			

六、报价文件

报价一览表

[货币单位：人民币/元]

项目名称：XXXXX

项目编号：XXXXX

序号	货物名称	品牌、产地	型号规格	数量	单价	总价	备注
合计	（大写）：				（¥ ）		

注：

1. 中文大写金额用汉字，如壹、贰、叁、肆、伍、陆、柒、捌、玖、拾、佰、仟、万、亿、元、角、分、零、整（正）等。
2. 所有价格均以人民币作为货币单位填写及计算。
3. 所有设备需详细列明。
4. 该表格式仅作参考，供应商的详细报价表格式可自定。

供应商名称（加盖公章）：

法定代表人（或授权代表）签字：

日期： 年 月 日

七、各类证明材料（如有）

1.采购文件要求提供的其他资料。

2.供应商认为需提供的其他资料。

3.测评服务方案（如有）
（根据本项目的需求，按照实际情况自行拟写，文字宜精炼、内容应具有针对性。）

4.质量保证措施（如有）
（根据本项目的需求，按照实际情况自行拟写，文字宜精炼、内容应具有针对性）

5.进度安排控制方案（如有）
（根据本项目的需求，按照实际情况自行拟写，文字宜精炼、内容应具有针对性）

备注：

本项目需提交纸质响应文件，响应文件截止提交时间为 2026 年 4 月 28 日 17:00，逾期不接收。

响应文件递交方式：现场递交或邮寄。（响应文件需密封，未密封拒绝接收）

联系方式:韶关市第一人民医院新区医院（武江区东景路 1 号）5 号楼行政楼 207 采购室 ；

联系人：黄小姐 ；联系电话：0751-8899272。