采购/调研文件

采购编号：_____

项目名称：_____

报名单位：_____

联 系 人：_____

联系电话：_____

报名时间：_____

盖　　章：_____

南昌大学第二附属医院招标采购中心

目录

南昌大学第二附属医院网络安全服务采购需求

一、项目概况

1、采购项目名称：南昌大学第二附属医院网络安全服务

2、采购数量：1 套

二、供应商资质要求

1.具有独立承担民事责任的能力；

2.具有良好的商业信誉和健全的财务会计制度；

3.具有履行合同所必需的设备和专业技术能力；

4.有依法缴纳税收和社会保障资金的良好记录；

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.法律、行政法规规定的其他条件。

7.所有不完整的投标将被拒绝；

8.投标人必须自行承担因其投标文件中的任何错漏而导致的一切后果；

9.本项目不接受联合体投标；

10.投标文件应在开标当天于开标时间前送至开标地点，逾期到达或不符合规定的投标文件恕不接受。

三、采购清单及技术参数

序号	服务名称	服务参数	输出物	服务量
1	互联网资产发现	1、在一年项目服务期内通过数据挖掘和调研的方式确定采购人信息资产范围，基于 IP 或域名，采用 WEB 扫描技术、操作系统探测技术、端口的探测技术、服务探测技术、WEB 爬虫技术等各类探测技术进行主动发现； 2、探测范围包含采购人信息系统内的主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等； 3、探测生成资产及应用列表，列表中包括设备类型、域名、IP、端口，更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。	《互联网资产发现报告》	四次
2	渗透测试	1、在一年项目服务期内针对采购人应用系统进行渗透测试两次（包含初测和整改后全面复测），测试对象应包括数据库系统、中间件、应用系统，以及身份认证等安全机制； 2、测试内容包括但不限于：根据网络脆弱性检测中发现的脆弱点，模拟黑客对系统中的终端、服务器进行现场渗透性验证； 3、测试方法包括但不限于 SQL 注入、XSS（跨站脚本）、CRLF 注入、代码执行、 目录遍历、文件包含、输入验证、认证、逻辑错误、密码保护区域猜测、字典攻击、特定的错误页面检测、脆弱权限的目录和危险的 HTTP 方法(如：PUT、DELETE) 等； 4、为保证过程安全可控，渗透测试工具为服务厂商自研； 5、渗透测试工具要求实现自动化渗透测试，贯穿整个渗透过程的操作，包括信息收集、指纹管理、漏洞发现、漏洞利用、后渗透攻击等模块。 6、渗透测试工具可根据编程平台提供的接口编写自己的攻击插件，实现自定义的攻击需求； 7、渗透测试工具可利用 http 协议、DNS 协议等远程获取外带数据；可通过内置的方法反弹交互 shell 到平台，执行 vim、交互执行操作等功能。	《渗透测试报告》 《渗透测试复测报告》	采购人指定的 30 个应用系统

3	漏洞扫描	1、在一年项目服务期内利用漏洞扫描工具对采购人网络中的核心服务器及重要的网络设备，包括服务器、交换机、防火墙等设备进行安全漏洞检测和分析； 2、对识别出的能被入侵者用来非法进入网络或者非法获取信息资产的漏洞，提醒安全管理员，及时完善安全策略，降低安全风险。	《漏洞扫描报告》	四次
4	风险评估	1、在一年项目服务期内对采购人信息系统开展整体风险安全评估，风险评估服务从管理层、网络层、系统层、应用层等多角度审查,全面而系统的评估采购人的安全状况，识别安全威胁与脆弱性,分析与监管要求的差距； 2、评估方法包括不限于：访谈、配置核查、实地勘察、渗透测试等，评估完成后，出具评估报告（含整改建议）。	《信息安全风险评估报告》	一次
5	重要时期安全保障服务	1、在一年项目服务期内的两会、国庆、HW 演习等重要时期为采购人提供 7*24 小时网络安全保障，通过积极防御、实时检测、响应处置等安全服务，提高组织的网络安全保障能力，保障重要时期信息系统安全稳定运行； 2、在重大活动开始前开展准备工作，包括但不限于协助采购人重保期间队伍组建、开展各项网络安全检查、协助整改及问题跟进、应急预案编制与演练等工作； 3、在重大活动期间，主要为采购人提供安全值守保障及技术支撑工作，负责重保期间采购人网络安全状况的监测、分析、研判、应急处置等工作； 4、在重大活动结束后进行总结工作，服务商对重保各环节工作中的优点与不足之处归纳总结，吸取经验教训指导采购人后续重保工作的优化和完善。	《重要时期安全保障服务方案》《重要时期安全保障日报》《重要时期安全 保障总结报告》	一年
6	威胁检测与响应服务	1、服务商在服务期内提供云端 SAAS 平台，实时接收并检测医院上传的安全告警与网络流量，通过云端 SAAS 平台向采购人提供 7*24 小时的威胁检测与响应服务，威胁检测与响应服务范围为医院内外网全流量且平台具备用户可视化页面。 2、保障服务期内的态势感知平台设备正常运转，定期巡检流量采集状况、存储情况、授权、规则和情报更新状态等，避免故障和异常影响设备威胁检测能力。为保障设备安全监测能力，服务人员定期对设备进行威胁情报、规则库进行更新，对系统进行版本升级。为保障云端运营平台及服务工具正常运转，日常巡检发现设备故障后，服务人员协调跟踪产品售后人员对设备进行故障修复； 3、7*24 小时监测，对网络内的安全隐患情况、外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况进行分析，对相关攻击事件及异常行为进行响应。监测范围需包含：APT 告警、恶意软件告警、网页漏洞利用告警、网络攻击告警、WebShell 告警等； 4、研判分析，云端服务团队通过远程运营平台监测到的告警，提供研判分析服务，分析内容需包括：APT 告警、恶意软件告警、网页漏洞利用告警、网络攻击告警、WebShell 告警等； 5、资产收集与录入，对采购人提供的资产进行识别、整理、记录和汇总。方便分析研判定位排查； 6、服务报告，服务人员对安全监测发现的安全隐患及事件在服务规定时间内进行通告，同时根据采购人需求每日同步安全	《服务周报》《服务月报》《服务年报》	一年

		情况。建立工作群推送告警信息，包括高频攻击源、恶意软件IOC 、内外交互的恶意链接等，需提供每日安全简报、服务周报、服务月报等相应服务报告； 7、安排资深专家在线进行运营情况汇报，进行威胁分析情况解读，并对安全运营中的产品问题、安全分析疑难问题进行解答，协助进行问题解决。 8、联动处置，对于态势感知平台同一品牌的防火墙、终端安全等产品，可通过安全运营平台对上述情况进行联动封禁，阻止进一步攻击； 9、为保证本地数据的安全性，平台需支持数据脱敏、加密后接入云端平台。		
7	应急响应服务	1、在一年项目服务期内对突发问题实现 7×24 小时响应制，发生或可能发生安全事件时，应急响应实施人员应快速响应并在 1 小时内到达现场，协助进行安全事件处理，及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏； 2、应急响应实施人员不能在时限内解决问题，则应调动后台安全专家协助解决，直到安全事件排除； 3、事件处理结束后，协助用户检查所有受影响的系统，追查 事件来源，在准确判断安全事件原因的基础上，提出基于安 全事件整体安全解决方案，协助后续处置。并根据要求完成应急响应报告。	《应急响应报告》(按照服务期内发生安全事件数量提交报告)	一年
8	安全预警通告	1、在一年项目服务期内以邮件或当面沟通形式向用户通告业内安全态势、重大舆情信息、重要系统漏洞及补丁信息等； 2、对于紧急重大类漏洞信息，以最快时间通过邮件或电话向采购人告知漏洞危害、影响范围及应对方案等信息； 3、通告内容应来自各主流厂商、安全研究组织以及企业安全团队所提供的安全漏洞信息、安全新闻、安全研究报告等。	《安全热点周报》(每周一份) 《安全预警通告》(按照服务期内安全预警事件实时发送)	一年
9	网站云监测	服务期内依靠网站安全监测平台对南昌大学第二附属医院重要互联网业务系统开展 7*24 小时的安全监测，主要包括可用性监测、黑词、黑链监控、篡改监控、挂马监控、DDOS 攻击、并对 Web 网站开展定期漏洞扫描。	《网站安全监测报告》	5 个互联网业务网站
10	攻击队评估服务	1、在一年项目服务期内通过专业攻防团队组成攻击队，采用模拟黑客 APT 攻击的方式，在不对业务系统造成破坏的前提下，不限定攻击路径和手段，以系统提权、控制业务、获取数据为目标； 2、针对采购人信息系统、人员、软件、硬件和设备同时执行的多混合，基于对抗性的模拟攻击，以此来发现系统、技术、人员和基础架构中的存在的隐患，深入评估采购人网络安全防护短板； 3、攻击队评估测试周期不少于 2 周，参与攻击队评估人员需具备国家级、省级大型攻防演习实施经验。	《攻击队评估报告》	一次
11	应急演练服务	1、在一年项目服务期内开展应急演练服务，根据真实常见的网络安全事件，通过对事件发生原理、过程、应急响应处置思路、内容归纳总结，结合采购人《网络安全应急预案》制定演练方案； 2、演练内容包括但不限于：特定网络安全事件科普介绍、网络安全攻击演示、应急响应过程演练等内容； 3、通过演练，协助采购人检验单位预案，查找预案中存在的	《网络安全应急演练方案》 《网络安全应急演练总结报告》	一次

		问题，并进行完善，以提高应急预案的实用性和实操性； 4、通过演练，协助采购人磨合机制，明确人员职责分工，完善应急机制，增强队伍应急响应能力		
12	协助优化策略	在一年项目服务期内，协助检查和改进防火墙策略，发现策略过宽、策略缺失、策略冗余、策略失效未废止等问题，并提出对应的防火墙策略优化建议。根据采购人现场安全设备威胁告警做研判分析，协助采购人调整安全设备的检测策略，消除已有的误报告警，提升安全设备威胁告警的准确率。	《服务报告》	一年
13	协助完善安全管理制度	1、在一年项目服务期内，参照参照国家等级保护标准GB/T22239、GB/T22240及行业相关标准要求，对采购人网络安全管理现状进行评估，发现安全管理方面的薄弱环节； 2、针对发现的问题，为采购人提供安全管理制度具体优化建议，协助采购人落地并逐步完善日常安全管理制度。最终达成有序提升信息安全风险管控能力，保障信息系统安全运营的目标。	《服务报告》	一年
14	网络安全检查迎检服务	在一年项目服务期内，迎接监管机构或上级单位的网络安全检查或开展安全自查工作时，提供技术支持服务，具体工作包括：协助编制检查技术方案，配合开展安全检查及安全自查，汇总并分析安全检查结果，完成后续整改等工作。	《服务报告》	一年
15	服务器安全加固服务	在一年项目服务期内，给医院物理服务器/虚拟机/容器的提供服务器安全管理系统，依托于服务器安全管理系统的基础上提供主机安全加固服务。以防止感染勒索/挖矿病毒、弱口令密码、等保合规、服务器补丁空窗期被攻击等一系列有关服务器安全问题。 1、资产梳理服务：服务人员基于服务器安全管理系统，采集并梳理服务器的内部账户、进程、计划任务、软件应用、网络连接、端口、Web 站点、Web 服务、Web 框架、数据库、环境变量、启动服务、内核模块等多种资产类型，为后续的加固、防守、溯源分析提供支撑。 2、安全检测服务：服务人员基于服务器安全管理系统，采用多维度的基线核查，满足等保合规要求，准确识别服务器上存在的漏洞、后门、弱口令、风险文件、病毒、木马等各类风险威胁。 3、高危账号排查：服务人员基于服务器安全管理系统，检测克隆账号、隐藏账号、默认禁用的账号被启用等风险账号。 梳理出风险账号的名称、风险类型、是否可交互登录、UID/GID、管理员权限、账户所属组、Shell、远程登录、Home 目录、账户状态、是否域账户、是否登陆过、最近登录时间、最近登录IP、最近登录终端、最近密码修改时间、密码到期时间、账户到期时间等参考信息；从服务器维度统计分析风险账户数量。 4、主机加固服务：通过内核驱动对服务器进行全方位立体化加固，可对非法提权、恶意代码执行、加载无数字签名的驱动、系统文件篡改、页面篡改进行有效防护， 实现系统层面、应用层面的安全预警与立体化防御。 5、未知威胁防护：安全服务人员通过服务器安全管理系统在不依赖特征库的情况下可以识别出未知 WebShell、未知 SQL 注入漏洞、 未知上传漏洞等攻击行为并进行防护 。 在不依赖特征库的情况下可提供 Struts2 漏洞利用防护、 反序列化漏	《服务报告》	一年

		洞利用防护 、任意文件读取漏洞防护、 命令执行漏洞防护 、T3 协议漏洞防护等漏洞防护能力。 6、全流程安全防护：运用自适应防护技术、内核驱动技术，实现对网络层、应用层、系统层进行防端口扫描、防暴力破解、网页防篡改、无文件攻击等纵深防御。 7、完整攻击事件回溯：采用行为学习与分析技术，智能分析系统可疑行为， 自动生成系统访问、用户操作等行为日志，从攻击源、执行操作、访问对象角度形成完整访问攻击路径，方便用户事后回溯取证。		
16	敏感信息泄露情报服务	在一年服务期内以攻击者视角，聚焦于排查采购人的敏感信息泄露情况的情报服务，排查范围覆盖互联网及暗网的各种信息泄露渠道，覆盖范围包括：仿冒网站、账号口令、源码信息、文档信息、人员信息、社交平台、暗网泄露信息（可选）等，服务探测范围覆盖互联网及暗网的各种信息泄露渠道，一次服务、全网情况一网打尽，覆盖互联网各类公开应用（如搜索引擎、代码托管平台、网盘等）及主流暗网平台。	《敏感信息泄露排查报告》	两次
17	APP 安全评估	在一年服务期内开展 1 次 APP 安全评估服务，重点在于通过对采购人端安全、通讯及传输安全、服务端接口安全等多个层面进行细致的梳理、测试和分析，发现移动 APP 面临的安全风险。移动 APP 安全评估主要针对 APP 客户端漏洞和对应的 APP 服务端进行安全测试。其中客户端的安全测试包括移动 APP 自身出现的漏洞和移动 APP 所调用的系统组件漏洞。服务端的安全测试包括传输安全测试和服务端应用安全测试。	《APP 安全评估报告》	采购人指定的 APP
18	API 渗透测试	在一年服务器内开展 API 安全测试服务，主要通过 API 资产梳理、重要接口渗透测试，持续保护客户 API 安全，解决 API 资产不清、API 攻击识别、API 数据泄露无感知、API 安全管控无解决方案的问题。服务内容涵盖：安全配置测试、API 身份认证和授权测试、API 输入输出测试、业务逻辑安全测试、敏感数据保护测试、第三方框架/组件测试。	《API 渗透测试报告》	采购人指定的三个应用系统的 API
19	个人信息隐私合规评估	依据中央网信办、工信部、公安部、市场监管总局颁布的《APP 违法违规收集使用个人信息行为认定方法》、《APP 违法违规收集使用个人信息自评估指南》、工信部 337 号文等规范要求，对 APP、小程序的隐私数据保护合规情况通过工具及人工相结合的方式进行检测评估，检测移动 APP、小程序收集使用个人隐私信息行为、隐私政策条款（如使用规则、保存规则、用户权利等方面）等方面的内容。评估系统隐私政策的规范性、独立性、完整性、真实性等是否符合要求；评估系统行为是否符合隐私政策要求与个人隐私标准，包括权限检测、行为检测、隐私信息收集、隐私保护不当等；检测内容需涵盖:隐私政策完整性检测、与应用行为的实质符合检测、非必要信息收集检测、数据出境、第三方收集、隐私泄漏风险、使用权限检测等。	《隐私合规检测报告》	采购人指定的 APP、小程序
20	弱口令专项排查	检查采购人业务系统、服务器、网络设备、数据库、中间件等是否存在空口令或弱口令帐户，是否可通过该弱口令帐户登录；是否存在默认口令未修改，可使用默认口令进行登录设备。	《弱口令专项排查报告》	四次

四、商务条款

（一）服务要求：

1、为严格保障项目交付质量，本项目明确要求由投标人所投服务厂商直接派遣人员完成交付，且由同一服务厂商完成交付，不得分包。严禁以任何形式使用代理商及其关联方人员参与项目。项目团队进场前，需对拟进场人员的资质证明、所投服务厂商为其缴纳的社保记录及身份证信息进行全面核验。
2、项目整体服务期一年，服务期内，如果提供的系统发生故障，中标供应商须调查故障原因并上门免费修复直至满足系统性能的要求，或者更换整机或部分有缺陷的组件和材料。服务期内中标供应商应对由于设计、工艺或材料的缺陷而发生的任何不足和故障负责任。
3、中标供应商必须对其所提供的系统或服务及采用的相关技术进行免费现场培训，以满足使用单位在日常使用、操作等方面的需求。因培训而产生的一切费用均由中标供应商承担。
4、投标人所投服务厂商需为本项目配备一名唯一的项目经理和一名技术经理。
4、乙方在进行服务清单第 5、14 项服务内容即重要时期安全保障服务、网络安全检查迎检服务工作时,如甲方重保期间发生网络安全事故或者因网络安全问题被通报或者 HW 行动被扣分的，经甲方综合判断事故或问题原因为乙方工作失误造成，甲方有权对乙方进行扣款。每发生一次网络安全事故，对乙方罚款 1500 元;每一条重大通报问题对乙方罚款 1500 元;护网行动没拿到优秀防守单位，对乙方罚款 1500 元，最高可扣款 15000 元。

（二）付款方式：

1、签订合同后 15 个工作日内甲方支付乙方合同签约总价的 30%。
2、乙方在服务清单第 2、4、10、18、19 项服务内容即渗透测试、风险评估、攻击队评估服务、APP 安全评估、个人信息隐私合规评估完成后向甲方申请进度付款，经甲方确认交付物后，由甲方在 15 个工作日内向乙方支付合同签约总价的 30%。
3、乙方在一年服务期满后向甲方申请考核，按照考核要求进行付款，评分在 85 分以上为合格，支付合同签约总价的 40%；如评分不足 85 分，每降一分，扣除 2%的合同金额。甲方应在 30 个工作日内向乙方完成支付。甲方付款前，乙方应向甲方开具相应金额的税务发票,否则甲方不承担由此造成的延期支付责任。（考核表见附件 1）

五、评分标准

价格评分（30 分）		
评分点	**评审内容**	**分值**
价格评分	价格分采用低价优先法计算，即满足采购/调研文件要求且价格最低的响应报价为评标基准价，其价格分为满分。 其他响应供应商的价格分统一按下列公式计算： 响应报价得分=（评标基准价/响应报价）×30%×100（保留两位小数）	30 分
技术评分（52 分）		
评分点	**评审内容**	**分值**
技术符合性评审	供应商完全满足采购/调研文件“采购清单及技术参数”的全部内容，任意一项不满足作无效投标处理。 **评审依据：技术响应表/偏离表。**	/

服务工具保障	1.投标人在服务期内提供威胁情报平台供采购人（用户）使用，满足加 4 分，否则不加分。 **评审依据：响应文件中提供承诺书原件并加盖投标人公章，不满足要求不予加分。** 2.投标人在服务期内提供漏洞扫描服务工具供采购人（用户）使用，满足加 4 分，否则不加分。 **评审依据：响应文件中提供承诺书原件并加盖投标人公章，不满足要求不予加分。** 3.投标人在服务期内提供资产测绘平台供采购人（用户）使用，满足加 4 分，否则不加分。 **评审依据：响应文件中提供承诺书原件并加盖投标人公章，不满足要求不予加分。**	12 分
技术方案	投标人为本项目制定技术方案，方案包含：①项目背景、②服务内容（包含服务流程、服务产出物）、③项目管理、④项目人员安排。 每有一项内容完全符合本项目采购需求的，该项内容得 5 分；每有一项存在内容缺陷的，该项内容得 3 分；每缺一项内容的，该项内容不得分；最高得 20 分。 内容缺陷是指：方案阐述的内容仅罗列了上述要点，没有进行相应的说明、缺少具体的实施措施，方案内容有明显缺失、描述内容不规范、不清晰、不具备可行性等情况。 **评审依据：响应文件中根据投标人提供的技术方案进行评分。**	20 分
服务厂商漏洞挖掘能力	1.投标人所投服务厂商须在互联网上自建独立运营的漏洞响应平台，以便及时向用户进行漏洞预警通告。漏洞响应平台上拥有 6000 家以上的企业运营经验，白帽专家 9 万人以上，满足加 5 分；漏洞响应平台上拥有 3000 家以上的企业运营经验，白帽专家人员 5 万人以上，满足加 3 分；其他不加分。 **评审依据:响应文件中提供“漏洞响应平台”计算机软件著作权登记证书，服务企业数量截图、漏洞平台白帽专家人员基数数量截图、并提供链接地址加盖服务厂商公章佐证，否则不得分。** 2.投标人所投服务厂商具有自主漏洞挖掘能力，以便及时向用户进行漏洞预警通告。根据国家信息安全漏洞享平台(CNVD)发布的从 2024 年“支撑单位工作贡献”，服务厂商支撑工作年度贡献值为 3 万个以上的得 5 分;服务厂商支撑工作年度贡献值为 2 万个以上到 4 万个（含）的得 3 分；服务厂商支撑工作年度贡献值为 1 万个以上到 2 万个（含）的得 1 分，其他不得分。 注：国家信息安全漏洞共享平台官网链接：https://www.cnvd.org.cn/ **评审依据：响应文件中提供 CNVD 官网的截图并加盖服务厂商公章，不提供不得分。** 3.投标人所投服务厂商具备漏洞技术分析及重大漏洞事件响应能力，其在 2024 年 CNVD 技术组支撑单位能力评价中，于漏洞信息收集、原创漏洞挖掘、漏洞大数据支撑、漏洞技术分析、重大漏洞响应和集体任务协作六个能力象限中，总计获得 9 星得 1 分、10 星得 3 分、11 星及以上得 5 分，其他不得分。 **评审依据：响应文件中提供 CNVD 颁发的证明材料并加盖服务厂商公章，不提供不得分。**	15 分
项目经理	投标人所投服务厂商为本项目配备的唯一项目经理需具备 10 年以上工作经验（以毕业时间为准），本科及以上学历、信息安全或计算机	5 分

	相关专业，不满足不得分。须具备以下资质，全部满足资质 5 分，最低得 0 分。 1.项目经理须具备注册信息安全专业人员认证（CISP）或信息系统安全专业认证（CISSP），项目管理专业人员(PMP)或中国项目管理师（CPMP）资质证书，符合条件得 3 分，不符合得 0 分； 2.在满足以上要求的基础上，项目经理如具备注册渗透测试专家（CISP-PTS）或注册数据安全治理专业人员（CISP-DSG）资质证书的，每个证书得 1 分，最高得 2 分，不具备得 0 分； **评审依据：投标人需提供项目经理简历、毕业证书、资质证书复印件，CNVD 原创漏洞证书复印件，及开标前 6 个月内任意一个月为其缴纳的社保证明料，并加盖所投服务厂商公章。**	
商务评分（18 分）		
评分点	**评审内容**	**分值**
商务符合性评审	供应商完全满足采购/调研文件“商务条款”全部要求，任意一项不满足作无效投标处理。 **评审依据：商务响应表/偏离表。**	/
服务厂商履约能力	自 2023 年 1 月 1 日至今（以合同签订时间为准），投标人所投服务厂商每具有一个类似安全服务合同案例得 2 分，此项最多得 6 分。 **评审依据：响应文件中提供江西省内安全服务合同原件的扫描件或复印件并加盖所投服务厂商公章，合同名称或正文应包含“安全服务”或“安全防护服务”或“重要时期网络安全保障”或“渗透测试”关键字，安全设备类及其他类合同不得分。**	6 分
服务厂商资质	1.投标人所投服务厂商具有中国国家信息安全漏洞库(CNNVD）认证资质，属于核心技术支撑单位的得 1 分，其他不得分。 **评审依据：响应文件中提供有效期内的证书复印件并加盖所投服务厂商公章，不提供不得分。** 2.投标人所投服务厂商具有 CCRC 信息安全服务资质-软件安全开发（一级）证书，得 3 分；（二级）证书得 2 分；（三级）证书得 1 分 注：安全服务资质-软件安全开发：一级>二级>三级。 **评审依据：响应文件中提供以上证书复印件并加盖所投服务厂商公章，不提供不得分。** 3.投标人所投服务厂商具有 ISO28000 供应链安全管理体系认证及 ISO27701 隐私信息管理体系认证，每具备一项证书得 2 分，此项最多得 4 分。 **评分依据：响应文件中提供以上证书复印件并加盖所投服务厂商公章，不提供不得分。** 4.投标人所投服务厂商具有信息安全服务资质（安全工程类三级）证书，信息安全服务资质（安全开发类二级），每具备一个证书得 2 分，此项最多得 4 分。 注：安全服务资质安全工程类证书级别：三级>二级>一级；目前最高级别为三级； 安全服务资质-安全开发类证书级别：二级>一级 目前最高级别为二级； **评审依据：响应文件中提供以上证书复印件并加盖所投服务厂商公章，不提供不得分。**	12 分
合计		**100 分**

附件 1：运行维护服务项目服务评价考核表

运行维护服务项目服务评价考核表

序号	考核项目	分值	考核标准	得分
1	人员结构 人员管理	20	乙方应该按照合同要求提供具有相关专业认证并符合相关工作经验要求的安服人员进行安全服务。需要进行现场办公的，按照甲方要求进行现场管理。人员不满足专业认证要求或者工作经验要求的每人次扣 5 分。扣满为止。 乙方备案进场人员如违反甲方现场管理规定（例如着装不整齐、被甲方用户部门投诉并经核实记录在案等情况），由甲方不定时抽查，每发生一次扣 5 分。扣满为止。	
2	应急响应	30	1）一般安全事件工程师未及时响应，一次扣 1 分； 2）重大安全事件未及时响应，一次扣 5 分；故障造成业务中断的，未按客户要求赶赴现场响应的，一次扣 10 分；	
3	安全管理	30	1）各设备登录未进行账号密码保护，经抽检发现一台扣 5 分； 2）因安服人员原因影响业运行务速度的，一次扣 2 分；未经客户允许，因人为操作因素造成业务中断，一次扣 10 分； 3）安服人员管理自己的账号密码，严禁使用弱密码，发现一次扣 5 分； 4）未经甲方同意私自开 vpn、堡垒机账号、设备账号、服务器端口号等，经发现一次扣 5 分。	
4	其他要求	20	不能出现利用工作便利泄露客户信息、客户数据等情况，每出现一起，视情节严重性扣 5-10 分；	
5	服务质量	加分项	1）安全服务人员协助甲方解决工作以外的重大问题，视情况加 5-20 分； 2）获得通报表扬、科室表扬信，经客户认可后，一次加 2 分； 3）加分后总分不超过 100 分。	
合计：				

六、文件编制要求

1. 采购/调研文件的组成和要求

1.1 投标人应报送的采购/调研文件的具体内容和编排顺序如下：

0.采购/调研文件封面；采购/调研文件总目录或索引（总目录或索引格式由申请人自行设计）；

1.投标人致函（附件 1）；

2.授权书（附件 2）；

3.承诺函（附件 3）；

4.中小企业声明函（附件 4）；

5.投标人资格要求（复印件加盖公章）；

6.投标人须提供售后服务能力承诺证明材料（南昌地区）；

7.报价单；

8.需求响应/偏离表；

9.技术文件；

10.投标人认为有必要提供的其他资料；

11.投标企业情况一览表；

1.2 投标人应编写采购、调研文件目录及页码

1.3 投标人提交的采购/调研文件应客观、属实。如投标方无故不参加投标活动或迟到 2 次以上（1 年内）、提供虚假材料、近三年内经营活动中有重大违法记录、采取不正当手段诋毁或排挤其它投标人、恶意串通或行贿、拒不签订或不如实履行采购合同、无事实依据恶意投诉，或有其它违法违规行为干扰招标活动的，招标人有权取消投标申请人的投标资格，并将该投标单位列入黑名单，3 年内不得参与我院任何采购项目投标。如果招标人因此遭受损失，投标人应予以赔偿，并且承担相应的法律责任。

2. 采购/调研文件的形式和签署

2.1 采购/调研文件：电子文件应扫描已加盖公章文件；纸质文件应加盖公章，左侧装订或胶装（如果申请文件太厚，可以分册装订），装订方式应牢固、美观，不得采用活页方式装订。

3. 采购/调研文件的递交审核

3.1 投标人应在规定的时间内，在南昌大学第二附属医院采购管理平台网站上传资料（网址：https://bid.jxndefy.cn/home）。

3.2 招标人有权拒绝接收在本条规定的截止时间以后收到的以及未递交到本条规定网站或地点的任何采购/调研文件，被拒绝的采购/调研文件将原封退还投标申请人。

3.3 投标人采购/调研文件申请通过后，本项目以投标人在南昌大学第二附属医院采购管理平台网站（网址：https://bid.jxndefy.cn/home)上传的采购/调研文件为依据进行评审。

仅当南昌大学第二附属医院采购管理平台网站（网址：https://bid.jxndefy.cn/home)出现故障情况下，按投标人递交的纸质采购/调研文件为依据进行评审。未递交纸质采购/调研文件的投标人，按无效处理。

3.4 投标人应准备一份采购/调研文件正本和六份副本，每套采购/调研文件须清楚地标明“正本”或“副本”。若正本和副本不符，以正本为准。

4. 项目技术参数（所投项目完全符合或满足临床要求）

5 评审办法

5.1 采用综合评分法，在满足资格及科室需求的情况下，所有专家评分中综合得分最高者为成交单位。

6 注意事项

6.1 当事人认为采购/调研文件、议价过程和成交结果使自己权益受到损害的，应当在以下规定时间内以书面形式向招标采购中心提出质疑。

对采购/调研文件提出质疑的，为资格审核通过之日起三日内，超出规定时间不予受理。

对议价过程提出质疑的，为各议价程序环节结束之日起三日内，超出规定时间不予受理。

对成交结果提出质疑的，为成交结果公示期限届满之日，超出规定时间不予受理。

1. 投标人致函（附件 1）；

投标申请人致函

致：南昌大学第二附属医院：

在充分研究上述招标项目之采购/调研文件中规定的要求和条件后，我们谨此向你们递交_____（项目编号及名称）采购/调研文件，并以此文件作为上述招标的合格投标人。

我们承认你们指定的代表有权为证实我们递交的声明、文件及资料或验证我们的财务和技术状况进行调查。为此，我们授权任何相关的个人或公司向你们提供所要求的和必要的真实情况和资料以证实我们在采购/调研文件中所填报的各项内容。

我们在此郑重承诺：如果在该项目投标过程中或者在中标后，招标人或者有管辖权的招标投标行政监管机构发现并查实我公司在所填报的该项目采购/调研文件中存在提供虚假或不真实的信息或者伪造数据、资料或证书等情况，不管招标人或有管辖权的招标投标监管机构是否有合法的处罚依据，我公司将无条件地自动放弃该项目的投标资格和中标资格；如果我公司已经收到中标通知书，我公司无条件地承认，我公司所收到的该项目中标通知书为无效文件，对招标人不具任何法律约束力；由此造成的任何后果和损失均由我公司承担。

本段承诺具有相对独立性，不管是否有其他相反的说明，本段承诺是我公司获得投标资格后所递交的采购/调研文件的有效组成内容，是我公司真实意思的表示，对我公司在与该项目有关的任何行为中始终具有优先的法律约束力。

我们完全理解并接受你们在采购/调研文件中关于上述招标项目之采购/调研文件的所有安排以及你们根据情况需要可能做出的适当调整。

如你们需要我们提供任何进一步资料，请与下述人员联系：

姓　　名:_____

联系电话:_____

地　　址:_____

我们声明，我们所填报的资料是完全真实和准确的，并愿为此承担任何法律责任。

投标申请人（公司名称及公章）：

法定代表人或授权委托人（签字或盖章）：

日期：

2. 授权书（附件 2）；

授权书

本人_____（身份证号：_____），作为（公司名称）_____法定代表人，在此授权我公司_____先生/女士（身份证号：_____）作为我公司正式合法的代理人以我公司名义并代表我公司全权处理_____（项目编号及名称）招投标业务办理及合同签订等相关事宜。

本授权书限期自_____起至_____止（期限不少于一年）。

在此授权期限内，被授权人所实施的行为具有法律效力，授权人予以认可。

_____（公司名称及公章）

法定代表人（签字或盖章）：

日期：_____

授权人身份证复印件正面	**授权人身份证复印件反面**
被授权人身份证复印件正面	**被授权人身份证复印件反面**

3. 承诺函（附件 3）；

承诺函

南昌大学第二附属医院：

我公司郑重承诺在本次采购活动中，所提交的材料是真实、有效的，复印件与原件一致的。

不存在借用、挂靠资质，围标、串标等违法违规行为；不存在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，参加同一合同项下采购活动的情况；不存在属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加采购活动的情况。

如隐瞒有关情况或提供任何虚假材料，我公司自行承担一切法律后果。我公司将自觉接受接受招标人、投标单位、广大群众监督，若发生违诺行为，自愿接受任何处罚。

_____（公司名称及公章）

承诺人（签字、盖章）：_____

日期：_____

4. 中小企业声明函（附件 4）；

中小企业声明函（工程、服务）

本公司郑重声明，根据《保障中小企业款项支付条例》（中华人民共和国国务院第728号）的规定，本公司参加南昌大学第二附属医院的*（项目编号、项目名称）*议价活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。本企业的具体情况如下：

1.*（标的名称）*，属于_____行业；本企业从业人员____人，营业收入为____万元，资产总额为____万元，属于*（中型企业、小型企业、微型企业）*；

2.*（标的名称）*，属于*工业*行业；本企业从业人员____人，营业收入为____万元，资产总额为____万元，属于*（中型企业、小型企业、微型企业）*；

……

本企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

注：

1、从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2、投标人应当对其出具的《中小企业声明函》真实性负责，投标人出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标。

5. 投标人资格要求（复印件加盖公章）；

5.1.具有独立承担民事责任的能力；

5.2.具有良好的商业信誉和健全的财务会计制度；

5.3.具有履行合同所必须的设备和专业技术能力（相关业绩）；

5.4.有依法缴纳税收和社会保障资金的良好记录；

5.5.参加采购活动前三年内，在经营活动中没有重大违法记录；

5.6.投标单位应提供《企业法人营业执照》、《法人授权书》、《资质证明》、项目负责人及相关人员资质证书复印件等，开标需带原件校验。

5.7.提供“采购需求”涉及的相关材料。

6. 投标人须提供售后服务能力承诺证明材料（南昌地区）；

注：资格审核时第 7 至第 11 项不需提供。

7. 报价单；

报价单

项目编号_____

项目名称_____

序号	名称	数量	单价（元）	总价（元）	是否属于中小企业	备注
1						
2						
合计（大写）：						

注：1、投标人为中小企业须在明细表中注明，并在采购、调研文件中提供相应证明材料，否则产生的一切后果由投标人承担。

2、投标人必须填写分项报价，以证明投标报价的合理性，否则视为无效投标。

投标人盖章：

法定代表人或委托代理签字或签章：

8. 需求响应/偏离表；

序号	采购、调研文件条目号	招标需求	投标响应	响应/偏离	说明

注： 1、响应/偏离内容应在说明栏中说明该条款在采购、调研文件中（或页码）的依据；

2、投标人不按上述表格填写，所产生的一切后果由投标人承担。

投标人盖章：

法定代表人或委托代理签字或签章：

9. 技术文件；

内容包括：

1、服务内容的详细说明

2、投标人认为需要说明的其他内容（投标人视需要自行编写）

10. 投标人认为有必要提供的其他资料；

11. 投标企业情况一览表；

投标人名称						
注册地址				邮政编码		
联系方式	联系人			联系电话		
	传　真			网址/邮箱		
企业性质						
法定代表人	姓名		技术职称		电话	
技术负责人	姓名		技术职称		电话	
成立时间			员工总人数：			
营业执照号						
注册资金						
开户银行						
银行账号						
经营范围备注						