江南大学附属医院安全运营服务（运维类接续 2024）合同书

甲方（采购人）：江南大学附属医院

乙方（中标人）：江苏万和协创信息科技有限公司

一. 采购项目编号：JSZC-320200-PXGJ-G2025-0136

二. 采购内容：江南大学附属医院安全运营服务

三. 中标总金额：（大写）柒拾壹万玖仟伍佰元；（小写）719500.00 元

四. 质量和包装要求及验收标准：符合招标文件相关要求

五. 交货期或完工期：合同签订生效后一年

六. 交货地点和方式：江南大学附属医院南北院区

七. 货款支付步骤和办法：合同生效后，中标供应商开具有效发票后 30 日内采购人支付合同总金额的 30%；供应商按合同要求服务满 6 个月后，采购人根据半年度考核报告结果，支付合同总金额*50%*考核支付比例－合同总金额*30%；供应商按合同要求服务满 12 个月后，采购人根据第二个半年度考核报告结果，支付合同总金额的 50%*考核支付比例。

八. 售后服务：符合招标文件相关要求

九. 违约责任：详见合同条款（六）：违约责任

十. 解决争议的方式：见合同条款（九）合同生效及其它

十一. 其他事项：无

十二. 合同不可分割部分：

招标文件、投标文件、合同条款及中标通知书，乙方在投标、评标过程中所作其它有关承诺、声明、书面澄清等均为合同不可分割的部分，与主合同具有同等法律效力。

十三. 合同备案：

合同一式肆份，乙方壹份，甲方叁份（财务处、采购中心、主管职能部门各壹份）。

十四. 合同生效：

本合同由甲乙双方签字、盖章后生效。

甲方（采购人）：　　（盖章）　　乙方（中标人）：　　（盖章）

2025/12/30

2025年12月30日

江南大学附属医院 XB025044

法定（授权）代表人：

年　　月　　日

法定（授权）代表人：

年　　月　　日

乙方户名：江苏万和协创信息科技有限公司

乙方开户银行：宁波银行无锡锡东支行营业部

乙方账号：78160122000002930

江南大学附属医院-X202504

合同条款

根据江南大学附属医院编号 JSZC-320200-PXGJ-G2025-0136 招标文件和该文件的中标通知书及乙方投标文件，甲乙双方就此次江南大学附属医院安全运营服务及相关问题，同意按下列条款规定执行。

（一）合同内容： 甲方向乙方购买 安全运营服务 。

（二）价格及支付：

1. 按此次中标价格执行，合同总标的额为 719500 元。

2. 付款方式：合同生效后，乙方开具有效发票后 30 日内甲方支付合同总金额的 30%；乙方按合同要求服务满 6 个月后，甲方根据半年度考核报告结果，支付合同总金额*50%*考核支付比例－合同总金额*30%；乙方按合同要求服务满 12 个月后，甲方根据第二个半年度考核报告结果，支付合同总金额的 50%*考核支付比例。

（三）知识产权

乙方承诺拥有所提产品及配套软件、程序和知识库或其授予甲方的权利的全部知识产权，且保证所提供的产品及配套软件、程序和知识库或其授予甲方的权利不会侵犯任何第三人的版权、专利权或商标权等知识产权或其他权利，不违反任何第三方的信息专有权，也没有其他针对乙方所提供的软件、程序和知识库等权利的未决诉讼。甲方行使乙方所授予的软件权利不会侵犯任何第三人的合法权利。若乙方向甲方提供的软件、程序和知识库等存在或发生知识产权等纠纷，一切责任均由乙方承担，甲方不承担任何责任。如不可避免地造成甲方损失的，甲方有权向乙方追偿（该等损失包括但不限于损害赔偿金、甲方为解决纠纷支付的律师费、诉讼费、差旅费等合理费用）。乙方并应按照合同总价的 20%向甲方支付违约金，如给甲方造成其他损失的，乙方还应负责赔偿。

（四）工程实施：

1. 甲方按本合同约定内容进行服务，并为甲方提供培训服务。

2. 甲、乙双方应确定各方参与产品服务工作的人员及其职责，甲、乙方具体人员名单及职责在签订合同前必须书面明确，并确定交流及联系方式，以确保维护服务工作的顺利进行。

3. 乙方派遣至甲方服务人员，需遵守甲方工作纪律，未经甲方同意，乙方

江南大学附属医院-X2025041

不得擅自对服务人员进行调换。

4.在合同履行过程中，甲方有权利要求乙方进行岗位调配，对不能胜任或不符合业务要求的人员进行更换。乙方本项目人员入离职情况应及时书面报甲方备案。

5.服务要求

5.1 僵尸后门清理服务

服务内容：对重点保护主机进行针对僵尸后门的全面检测，形成专项扫描报告，针对检测出的问题进行清除处理，促进僵尸后门进行闭环处置。

服务频率：提供 1 年不少于 4 次僵尸后门清理服务。

交付成果：每次服务完成后 3 日内交付《后门清理总结报告》

5.2 攻击弱点加固服务

服务内容：现场服务工程师全面检测并协助加固系统漏洞、弱口令、高危服务等。检查系统配置，建立防爆破、权限控制等基本策略。收集各类型操作系统的漏洞补丁，检查各主机的系统和业务补丁加载情况，以及主机上的安全策略配置情况，针对发现存在不合理或者不完善的地方，首先现场进行解决。如果在现场不能解决的问题，将会以安全建议的方式提出，督促相关厂商进行实施。

服务频率：提供 1 年不少于 2 次攻击弱点加固服务。

交付成果：每次服务完成后 3 日内交付《专项安全加固报告》

5.3 安全配置合规保障服务

服务内容：基于医疗行业特点和安全基线规范基准的专业检查平台，用以上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查和安全服务任务中，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力和达到整体合规要求。安全配置合规保障，主要应用于设备入网、工程验收、日常维护、合规检查等方面。通过对目标系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险。

服务频率：提供 1 年不少于 4 次安全配置合规保障服务。

交付成果：每次服务完成后 3 日内交付《安全配置合规保障服务报告》

5.4 Web 漏洞暴露情况检查服务

提供 Web 漏洞暴露情况检查服务，周期性对指定的 Web 应用进行检测，分析其漏洞暴露情况以及是否暴露于互联网，全面覆盖 OWASP Top 10 等常见高风险漏洞。提供基础报告解读服务，协助快速理解当前安全状况和需优先关注的领域，并配合进行 web 漏洞全生命周期管理工作。

服务频率：提供 1 年不少于 4 次 Web 漏洞暴露情况检查服务。

交付成果：每次服务完成后 3 日内交付《Web 漏洞暴露情况检查服务》

5.5 防护能力提升服务

服务内容:提供对网络安全工具、服务器及业务系统的安全策略优化服务，定期巡查安全工具、服务器及业务系统的配置，验证现有安全访问控制策略是否起到作用、是否合理高效进行检查和改进，及时发现和控制风险，对于不合规的配置项执行通告机制，评估影响并协助调整策略优化。通过持续优化网络及系统架构、设置/调整网络防护策略，以实现有效提升防护质量、有效缩小暴露面。

服务频率：提供 1 年不少于 4 次防护能力提升服务。

交付成果：每次服务完成后 3 日内交付《安全防护提升总结》

5.6 渗透测试服务

服务内容：技术人员站在攻击者的角度、完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统（集成平台、HIS、LIS、PACS、体检、病理、心电、手麻以及新上线业务系统等系统）的安全状况做深入探测，检测系统是否存在信息泄露漏洞、配置管理漏洞、身份认证漏洞、输入验证漏洞、越权漏洞、会话管理漏洞、业务逻辑漏洞、组件漏洞等。

服务频率：1 年提供不少于 2 次渗透测试服务。

交付成果：每次服务完成后 3 日内交付《XXX 系统渗透测试报告》（包含漏洞修复建议）

5.7 安全评估服务

服务内容：安全评估主要使用专用的安全扫描工具和设备，以本地扫描的方式对集成平台、HIS、LIS、PACS、体检、病理、心电、手麻以及新上线业务系统等系统评估范围内的设备或系统进行安全评估，来查找系统的安全风险、漏洞和威胁。

服务频率：1 年提供不少于 4 次安全评估服务。

交付成果：每次服务完成后 3 日内交付《安全评估报告》

5.8 攻击诱捕服务

服务内容：提供攻击诱捕探针服务工具部署在现场，在入侵者必经之路上构造陷阱，混淆攻击目标，吸引攻击者进入陷阱，实现攻击捕获，延缓攻击者对实际业务网络的攻击，全程监测攻击轨迹和行为，实现攻击行为的快速取证溯源，保护真实网络资产，同时以技术分析手段实现对攻击者的追踪。

服务频率：提供服务工具实时监测。

交付成果：攻击诱捕系统（服务工具部署在用户现场，南、北院区各一套），每月 5 日前提供上一个月《攻击诱捕报告汇总》

5.9 未知威胁监测服务

服务内容：提供未知威胁发现系统服务工具部署在现场互联网 DMZ 区，利用沙箱技术实时检测、报警和动态响应，帮助网络管理员对特定威胁、未知威胁、恶意代码、隐秘通道、嵌套攻击等进行深度识别，找到网络中可能存在的隐患。

工具要求：服务工具满足如下能力：

1、提供对网络流量中主流协议进行识别、解析还原并记录，用于取证分析、威胁发现，支持协议包括：HTTP、DNS、SMTP、POP3、IMAP、Mysql、DB2、Oracle、SMB、NFS、FTP 等；支持对网络流量中的文件进行识别和还原，支持可执行文件、文档类文件、压缩文件、移动应用等。

2、支持对各种攻击类型进行统计，包含扫描器漏洞探测、敏感信息探测、网络扫描探测、PHP 代码执行、WEB 攻击扫描、路径穿越攻击、XSS 跨站脚本、SQL 注入攻击、二进制攻击、未知代码执行、SHELL 命令执行、JAVA 代码执行、JAVA 反序列化代码执行、STRUTS2 代码执行、域内渗透攻击等攻击类型统计。

服务频率：提供服务工具实时监测。

交付成果：未知威胁监测系统（服务工具部署在南院现场一套），每月 5 日前提供上一个月《未知威胁报告汇总》

5.10 资产梳理服务

服务内容：在之前资产梳理清单的基础之上，进行资产更新梳理，包括外网资产和内网资产。外网资产梳理主要针对外网资产进行发现并协助梳理，梳理内容包括互联网域名、IP、端口、服务、中间件、操作系统等。内网资产梳理主

要针对内网主机、服务器、应用，网络设备、安全设备等资产进行发现并协助梳理。

服务频率：提供 1 年不少于 2 次资产梳理服务。

交付成果：每次服务完成后 3 日内交付《资产梳理清单》

5.11 安全值守服务

服务内容：提供有丰富经验的工程师 1 人在采购人现场工作，提供现场和第一时间的问题咨询、故障诊断、协助处理故障、设备更换配合、安全事件处理、安全漏洞处理、系统安全状态维护、定期安全日志审计等。

服务频率：提供不少于 1 人驻场服务。

5.12 安全运营制度完善服务

服务内容：根据采购人实际需求及国家、上级部门相关最新政策文件要求，协助采购人进行信息安全相关制度修订或新增。收集、审阅采购人现行的信息安全相关制度、规定、办法、流程等文件，基于最新要求进行差距分析，对采购人现有但内容陈旧的制度进行修订或新增，确保其语言准确、流程清晰，并符合最新政策要求。针对当前制度体系的空白或薄弱环节，协助采购人补充全新的制度文件。

服务频率：提供 1 年不少于 1 次安全运营制度完善服务。

交付成果：提供修订与新增的《XX 制度》终稿。

5.13 安全通告服务

服务内容：由供应商收集并整理安全漏洞信息、病毒信息、安全预警信息，并给出相应的解决方案，并定期以邮件、电话等方式传递给采购人，并协助采购人根据解决方案进行漏洞修补。安全通告服务内容包括但不限于：厂商安全通告、其他安全通告等。

服务频率：服务期内按需响应提供。

交付成果：每次服务完成后 3 日内交付《安全通告文档》

5.14 网络应急响应服务

服务内容：基于面临的具体安全事件开展专家应急响应，安全事件检测、安全事件抑制、安全事件根除、安全事件恢复、安全事件总结，最终形成协调联动机制，增强应急技术能力，健全应急响应机制。安全事件处置完成，系统得到

江南大学附属医院-2025044

恢复，找到安全事件发生原因并提供安全解决方案，并提供安全事件应急响应报告。

服务频率：服务期内按需响应提供。

交付成果：每次服务完成后 3 日内交付《应急响应文档》

5.15 数据安全体系规划服务

服务内容：构建数据安全顶层设计体系，包括：规划数据安全治理组织架构与职责；制定数据安全战略目标与方针框架；设计数据分类分级管控方法论模板；建立数据安全风险评估基础流程模型；宣贯数据安全意识。通过体系化设计，为全面数据安全防护奠定战略基础，实现合规性提升。

服务频率：提供 1 年不少于 1 次安全体系规划服务。

交付成果：服务期结束前一个月内提交年度《数据安全体系规划》

5.16 安全培训服务

服务内容：根据采购人的实际需求，提供针对全员的信息安全意识培训，针对管理人员提供安全治理培训，针对技术人员提供安全攻防技术、安全开发、安全产品技术原理及安装部署等方面的培训。

服务频率：提供 1 年不少于 1 次安全培训服务。

交付成果：每次服务完成后 3 日内交付《安全培训报告》

5.17 安全事件响应服务

服务内容：快速响应病毒事件及前期可疑迹象，通过远程+现场相结合的安全专家级服务，迅速响应网内事件，覆盖检测、抵制、根除等关键动作。减少安全事件对业务影响时间、影响范围。

服务频率：服务期内按需响应提供。

交付成果：每次服务完成后 3 日内交付《病毒及威胁关联事件响应报告》

5.18 安全巡检服务

服务内容：由专业安全工程师定期针对服务器、数据库、网络设备和安全设备，进行策略的合理性和有效性检查，并对日志进行审计分析，记录保存检查和审计结果，并生成相应报告。

服务频率：提供 1 年不少于 4 次安全巡检服务。

交付成果：每次服务完成后 3 日内交付《巡检报告》

5.19 系统上线前信息安全监测服务

服务内容：资产登记备案： 新业务系统上线前，必须进行详细资产登记，明确系统边界、关键组件、责任人及网络位置等核心信息。

多维度安全审查：结合运用以下服务进行安全审查：

安全评估：对系统进行全量安全评估，识别已知安全风险。

基线核查：依据安全配置规范，核查系统与中间件的安全配置合规性。

渗透测试：在可控范围内，模拟攻击者进行深度渗透测试，挖掘逻辑漏洞与深层次风险。

风险整改与确认：对审查发现的高风险及中风险问题必须完成整改，并提供相关证据。最终需由安全团队确认系统符合入网安全基线要求。

安全入网：完成上述登记、审查、整改并确认安全后，方可正式接入网络运行，纳入常态化安全监控范围。

服务频率：服务期内按需响应提供。

交付成果：每次服务完成后 3 日内交付《上线前检测报告》

5.20 威胁阻断服务

服务内容：提供南院区、北院区 7*24 小时威胁阻断服务，旁路部署于互联网出口 DMZ 区，基于攻击诱捕、威胁监测分析结果，设置编排威胁监测拦截，无需依靠联动防火墙等边界设备，对恶意攻击者进行秒级拦截，保障业务安全运行。

服务频率：提供服务工具实时阻断。

交付成果：威胁阻断系统（服务工具部署在用户现场，南、北院区各一套）

5.21 数据安全风险评估服务

服务内容：系统化识别系统或项目核心数据资产面临的潜在风险。服务通过深度访谈、策略审阅、系统扫描与脆弱性检测，全面审视数据在采集、存储、传输、使用、销毁全生命周期的安全状况，验证现有防护措施如访问控制、加密、审计等的实际有效性。

服务频率：提供 1 年不少于 2 次数据安全风险评估服务

交付成果：每次服务完成后 3 日内交付《XX 系统数据安全风险评估报告》

（五）工程验收：

江南大学附属医院-X2025004

1.甲方根据国家有关规定、招标文件、乙方的投标文件以及合同约定的内容和验收标准进行验收。验收情况作为支付货款的依据。如有质疑，以相关质量技术检验检测机构的检验结果为准，如产生检验费用，则该费用由过失方承担。

2.若由于乙方的原因造成未能达到验收标准、甲方系统不能正常使用、工程停工、返工以及影响系统的正常运行等结果，甲方有权要求乙方限期进行整改，并由乙方承担所需的一切费用和对甲方造成的损失。

3.若由于甲方或其他系统报价人未能提供服务工作所必须的技术支持和配合，造成产品未能达到验收标准、甲方系统不能正常使用、工程停工、返工以及影响系统的正常运行等结果，乙方不承担任何责任。

（六）违约责任：

1. 甲方延期付款时（有正当拒付理由者或不可抗力除外），应向乙方偿付逾期付款违约金，计算方法：逾期支付款×2‰×逾期天数。违约金总额不超过合同相应项目的 5%。

2. 在履行合同过程中，由于乙方原因，未能达到合同条款规定的验收要求（除不可抗力外），应向甲方偿付逾期上线、运行、验收违约金。计算方法：合同总金额×5‰×逾期天数。如因乙方违约造成损失，甲方有权利要求乙方承担相应的损失。

3. 乙方在安装、维护中，甲方应提供便利，配合乙方技术人员正常工作。乙方技术人员经甲方授权后可以接触和使用用于安装、维护产品所必需的信息和设备，且不能泄露给第三方。由于乙方技术原因导致信息泄露由乙方承担全部责任，并且有义务免费完成程序修补工作，以避免此类事件的再次发生。甲方保留追诉乙方法律责任的权利。

4.如在服务期间，发现账号弱口令、越权访问、关键信息泄露等网络数据安全风险被国家、省、市等上级部门或网络安全主管部门通报的，查明是因乙方原因造成的，甲方被通报一次乙方应按照 3000 元/次向甲方支付违约金。通报超过三次的，甲方有权解除本合同，并要求乙方应按照合同总价的 10%支付违约金，如给甲方造成其他损失的，乙方还应负责赔偿。

5.乙方在接到甲方服务请求后，因客观原因未能在标准时间内提供相应服务，乙方应及时与甲方联系，在得到甲方同意的情况下重新定义响应时间，若无重新

江南大学附属医院-X2025044

定义或甲方不同意，按实际响应时间和标准响应比较，甲方有权扣除乙方因违约造成的相关违约费用，并由乙方承担甲方的相应损失，其中违约费用计算方法为：合同总金额×2‰×超出标准时间小时数（按合同的要求时间为始，到达现场时间为终）。甲方有权在乙方超出标准时间不能提供服务的情况下，另行委托第三方提供服务，并由乙方承担第三方的服务费用。如连续出现 3 次乙方未能在标准时间内提供相应服务，甲方有权利以乙方无法满足维护需求为理由无条件解除与乙方的合同，同时有权利要求乙方承担相应的损失。

6. 因不可抗力不能履行全部或部分合同的，经双方同意，应当免除遭受不可抗力一方的全部或部分委托责任。受不可抗力事件影响的一方应在不可抗力发生后不迟于十四个工作日内，将不可抗力事件的发生，预计延续的时间和终止时间书面通知另一方。

7. 上述“不可抗力”系指因不可归责于一方当事人之事由，如自然灾害、人害、战争、水灾、火灾、军事行动、法律改变、禁运、罢工等致不能或延迟履行本契约之任何规定时，该当事人毋庸对他方负任何责任与义务。

（七）终止罚款：

1. 如果发生下列情况，甲、乙各方有权单方面立即终止本合同：

⑴对方违约没有履行主要合同义务；

⑵未经甲方同意而拖延进行维护时；

⑶未经乙方同意将服务设备移出而继续要求服务时；

⑷违约拖欠乙方货款超过 30 日。

2. 因甲方违约而造成本合同的终止，乙方不退回合同款；因乙方违约而造成本合同的终止，甲方有权要求双倍退回未履行部分的合同款。

（八）保密责任：

甲、乙双方同意在本合同执行过程中了解到的与双方有关的内容以及数据或信息确认为机密。乙方未经甲方的书面许可，不得将甲方相关数据或信息用于其他目的，也不得以任何方式将其复制、传递给第三方。本合同终止或期满后亦同，但法律法规另有规定的除外。

（九）合同生效及其它：

1. 合同经甲乙双方代表签字并盖章后即生效。

2. 合同签订后甲乙双方即直接产生权利与义务的关系，合同执行过程中出现的问题应按照合同约定、法律法规的规定办理，在合同履行过程中，双方如有争议可协调解决。如协商不能解决，双方可向甲方所在地人民法院提起诉讼。

3. 合同在执行过程中出现的未尽事宜，双方在不违背本合同和招标文件的原则下协商解决，协商结果以书面形式签订补充协议，且补充协议与本合同具有同等效力。

4. 甲乙双方确认：对本合同条款及后果均已知悉，一致确认不存在欺诈、胁迫、乘人之危、重大误解、显失公平等任何可能导致合同无效或被撤销的情形。

5. 本合同的附件具有补充、解释或修改合同的作用，对合同双方有约束力。其他事宜按投标书承诺执行。

6. 合同附件

江南大学附属医院-X2025044

附件 1：服务考核及结果应用：

从签订合同生效之日起算，采购人每季度对供应商服务质量进行考核，考核完成后形成季度考核报告，并最终汇总形成半年度考核报告（半年度考核得分取对应两个季度考核结果的平均值）。半年度考核结果直接与服务合同付款金额挂钩，计算方式如下：

总分≥90 分，服务期内服务费支付比例为 100%；

80 分≤总分＜90 分，服务期内服务费支付比例为 90%；

70 分≤总分＜80 分，服务期内服务费支付比例为 80%；

60 分≤总分＜70 分，服务期内服务费支付比例为 60%；

总分<60 分的，当前服务周期采购人不再支付费用，同时采购人有权终止该服务合同。

考核类别	权重	考核子类	定义	完成指标	分数	考核要求	得分
服务团队	10%	服务范围	该指标考核供应商承诺服务范围	服务频率满足项目实施，招标要求，或与承诺的服务范围匹配。	2 分	根据问题的严重性分为三档 1）一般，扣 0.5 分； 2）较严重，扣 1 分； 3）十分严重，扣 2 分	
		服务人员技能	该指标考核供应商承诺的人员技能、沟通管理能力、组织协调能力	服务人员的技能、沟通和管理各项能力满足现场需求	2 分	根据问题的严重性分为三档 1）一般，扣 0.5 分； 2）较严重，扣 1 分； 3）十分严重，扣 2 分	
		服务人员工作纪律	该指标考核供应商提供的服务人员的工作纪律	服务人员的工作纪律好，不发生违反现场规定的行为	2 分	根据问题的严重性分为三档 1）一般，扣 0.5 分； 2）较严重，扣 1 分； 3）十分严重，扣 2 分	
		服务人员态度	该指标考核供应商提供的服务人员的服务态度	服务人员责任心强，服务态度好，积极展开相关工作	2 分	根据问题的严重性分为三档 1）一般，扣 0.5 分； 2）较严重，扣 1 分； 3）十分严重，扣 2 分	
		服务人员维护	该指标考核供应商提供的服务人员	服务团队的维护规范性，避免不必要的问题发生	2 分	根据问题的严重性分为三档 1）一般，扣 0.5 分；	

		规范性	的维护规范			2）较严重，扣 1 分； 3）十分严重，扣 2 分	
事件管理	40%	事件响应及时性	该指标考核供应商对网络安全事件的响应情况	事件响应 10 分钟，2 小时内开始处置。事件响应状态和结果及时通报采购人。	10 分	当月出现一次响应不及时或“未处置”事件，出现一次则不合格扣 1 分，本条目扣完为止。	
		事件处置结果	该指标考核供应商对网络安全事件的处置情况	网络安全事件需要在规定响应时间内处置完成，2 个工作日提供处置报告。	10 分	当月“待处置”或“未处置”事件出现一次或处置报告不满足要求则不合格扣 5 分，本条目扣分不设上限。	
		事件检测全面性	该指标考核供应商对网络安全事件的检测情况	服务期间需全面检测漏洞问题，防止漏洞通报或安全事件	20 分	服务期间出现因检测不到位导致的漏洞通报或安全事件，出现一次扣 5 分，本条目扣分不设上限。	
服务实施	30%	服务内容完整性	该指标考核供应商执行招标要求服务内容的完整性	服务内容需要按照服务范围、服务内容严格执行。	20 分	服务内容缺失或服务范围不足则不合格扣 10 分，本条目扣完为止。	
		服务内容交付成果	该指标考核供应商服务交付成果的质量。	服务执行结束提交对应服务工具，服务工具要符合用户实际情况。	10 分	服务工具缺失或交付质量差（不符合实际情况、无合理优化建议）则不合格扣 10 分，本条目扣完为止。	
服务管理过程	20%	项目实施	该指标考核供应商服务实施管理过程安排是否合理。	项目实施需要具有详细的实施方案、进度计划和人员安排。	6 分	实施方案缺失或项目进度计划缺失或无项目人员计划则不合格扣 3 分，本条目扣完为止。	
		项目汇报	该指标考核供应商日常报告提供的准时性	服务交付物按时提交，且质量满意	8 分	出现一次不及时扣 2 分，质量不满足要求扣 2 分，本条目扣完为止。	
		项目安全	该指标考核对现网业务系统影响	项目实施过程不应对现有系统产生宕机、正常业务中断等不利情况。	6 分	出现宕机、正常业务中断等不利情况每次扣 3 分，本条目扣分不设上限。	

附件 2：安全运营服务清单

序号	名称	服务频次	服务对象	采购要求说明
1	僵尸后门清理	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
2	攻击弱点加固	1 年不少于 2 次	江南大学附属医院全院信息资产	详见项目服务要求
3	安全配置合规保障	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
4	Web 漏洞暴露情况检查	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
5	防护能力提升	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
6	渗透测试	1 年不少于 2 次	江南大学附属医院全院业务系统	详见项目服务要求
7	安全评估服务	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
8	攻击诱捕	服务期内 7*24 实时监测	分别设置于南院区及北院区	详见项目服务要求
9	未知威胁监测服务	服务期内 7*24 实时监测	设置于南院区	详见项目服务要求
10	资产梳理	1 年不少于 2 次	江南大学附属医院全院信息资产	详见项目服务要求
11	安全值守服务	1 年	驻场于江南大学附属医院南院区	详见项目服务要求
12	安全运营制度完善服务	1 年不少于 1 次	江南大学附属医院	详见项目服务要求
13	安全通告服务	服务期内按需响应提供	江南大学附属医院	详见项目服务要求
14	应急响应服务	服务期内按需响应提供	江南大学附属医院	详见项目服务要求
15	数据安全体系规划服务	1 年不少于 1 次	江南大学附属医院	详见项目服务要求

16	安全培训服务	1 年不少于 1 次	江南大学附属医院工作人员、信息化管理人员	详见项目服务要求
17	事件响应	服务期内按需响应提供	江南大学附属医院	详见项目服务要求
18	安全巡检	1 年不少于 4 次	江南大学附属医院全院信息资产	详见项目服务要求
19	系统上线前信息安全检测	服务期内按需响应提供	江南大学附属医院新上线业务系统	详见项目服务要求
20	威胁阻断服务	服务期内 7*24 实时阻断	江南大学附属医院	详见项目服务要求
21	数据安全风险评估服务	1 年不少于 2 次	江南大学附属医院	详见项目服务要求

江南大学附属医院-X225044