广东医科大学顺德妇女儿童医院

（佛山市顺德区妇幼保健院）

项目需求书

项目名称： 2025 年度信息系统等保评测项目

2025 年 5 月

一、采购项目情况概述

随着信息化程度的越来越普及，而且国内外信息安全形式非常严峻，结合国家信息安全等级保护的安全要求，同时根据《信息安全等级保护管理办法》与佛山市相关网络信息安全文件的要求，本单位计划对已定级或初测的二级、三级信息系统进行信息安全等级保护测评工作。

二、项目采购内容

1. 项目清单

序号	项目名称	数量	单价（人民币元）	预算总金额（人民币元）	服务期限
1	2025 年度信息系统等保评测项目	1 项	400000	400000	合同签订之日起三个月内完成测评工作，至网络安全等级保护测评服务项目通过验收止。
合计：（单位人民币元）				肆拾万元整	
备注：					

三、项目实施地点：广东医科大学顺德妇女儿童医院

四、项目预算金额：合计不超过 400000 元人民币。预算中包括但不限于包含硬件购置费、测评费、整改费、实施费、安装调试培训费、人员支出（含差旅费等）、正版授权费用、税费等合同实施过程中应预见及不可预见费用一切费用。

五、项目要求

1.资质要求

（1）具备《中华人民共和国政府采购法》第二十二条规定的条件。

（2）必须是在中华人民共和国境内注册的具有独立承担民事责任能力的法人或其它组织。

（3）营业执照经营范围：本项目相关的内容。具有项目服务的能力，保证能及时对服务项目提供实施服务与建议。

（4）在近三年的商业活动中无违法、违规、违纪、违约行为；

（5）本项目不接受联合体参与，不接受转包、分包；

（6）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，不得参加同一项目报价,一经发现按废标处理并标记为不诚信供应商。

2.服务要求

（1）协助开展信息系统的定级备案工作，编写系统定级备案材料，获取公安部门颁发的备案证书；

（2）针对服务对象开展安全漏洞检测和差距测评，根据差距测评结果，给出针对性的整改建议；

（3）针对采购人受测信息系统的安全整改提供技术支持咨询工作；在采购人等保整改过程中，需提供免费咨询、顾问指导服务，以协助采购人在规定时间内完成等保整改。如采购人有需要，成交供应商需提供整改咨询会议。

（4）开展信息系统验收测评工作，出具《网络安全等级测评报告》；

（5）负责提交《网络安全等级测评报告》至公安部门审核，取得报告接收回执；

（6）协助组织召开网络安全等级保护定级评审会，协助定级评审专家邀请和专家评审费用及评审会议所有费用支出。

（7）协助做好信息系统备案工作，如有变更，协助相关备案变更手续办理。

（8）本项目在实施过程中所使用到的专业服务工具必须包含等级保护检查工具、网络边界完整性检查管理系统、网络安全事件调查处置工具箱系统、内网安全管理系统、等级保护合规检查工具箱等。本项目在实施过程中所使用到的专业安全测评项目管理工具，信息安全等级保护综合管理系统，该系统须通过公安相关部门的检测（响应时提供检测报告扫描件作为证明材料）。必须保证所使用的所有工具和软件不会产生所有权和知识产权纠纷，并保证工具和软件的可用性和可靠性，由此产生的一切责任由供应商承担。

3.技术要求

3.1 详细技术参数要求

说明：带“▲”号条款为评审时的重要技术参数，带“★”号条款为评审时

的一般技术参数，不作为投标无效条款。如中标后缺少整体架构所必需部件，均由中标方免费提供。

3.1.1▲信息系统等保评测

- 需测评系统清单：

序号	系统名称	系统等级	备注
1	HIS 系统	三级	年测
2	互联网医院系统	三级	年测
3	住院电子病历系统	三级	年测
4	医院信息集成平台	三级	年测
5	OA 系统	三级	年测
6	LIS 系统	三级	年测
7	PACS 系统	三级	年测
8	门户网站系统	二级	复测
9	产后母婴保健中心系统	二级	初测

供应商需协助采购人完成以上 9 个信息系统的等保测评相关流程工作，具体工作包含：

1、收集用户系统相关信息（资产清单、接口人、系统描述），联系测评机构。

★2、本期项目实施工期必须在是三个月内完成，供应商需保证在规定的时间内协助用户通过等保测评，并且拿到《网络安全等级保护等级测评报告》。

3、协助用户进行定级备案材料编写，如信息系统等级保护备案表，信息系统等保保护定级报告等。

4、配合测评机构，梳理测评过程和收集测评对象相关信息。

5、对于测评过程中发现的高风险项问题，及时与客户汇报沟通。

6、协调测评机构编写报告。

3.2★集成整改服务 1 项

1、供应商依据《信息系统安全等级保护测评要求》对本单位的信息系统安全等级保护状况评估，包括以下两个方面的内容：

（1）安全技术评估，主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个层面上的测评；

（2）安全管理评估，包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理评估。

若判定系统安全防护能力无法达到相应级别或要求，则提交《整改问题清单》。

2、供应商根据《整改问题清单》，提供技术手段协助用户进行安全整改。

3、参照《差距测评问题清单》协助甲方完成网络设备基线配置、网络安全设备基线配置、操作系统基线配置、操作系统补丁修复、数据库配置、管理制度文档。其中整改服务包括不限于：

（1）服务器安全加固服务

a.服务器操作系统的身份鉴别安全加固，配置登陆失败、操作超时、限制非法登录以及自动退出等；

b.配置服务器账号登录密码强度策略；

c.严格控制服务器操作系统的远程管理，限制远程管理终端，配置使用加密远程管理方式等；

d.对服务器操作系统账号的权限进行紧缩，遵循“最小权限”原则，防止对系统的越权访问；

e.清理不再使用、旧的系统账号；

f.禁用系统多余的、系统缺省打开却不必要服务系统服务，删除不再使用的共享；

g.开启系统日志审计功能，对系统事件的日期、时间、类型、主体标识、客体标识等进行记录，并定期分析；

h.配置服务器操作系统的防病毒及防恶意代码功能，安装防病毒软件，定期进行病毒查杀；

i.检查分析现有系统的安全漏洞和黑客后门等，更新服务器系统安全补丁；

j.对服务器操作系统的运行状态、系统服务等进行监控；

k.配置应用平台（IIS、apache 等）的安全参数，加强应用安全。

（2）关键网络设备加固

a.根据相关策略对设备进行检查与设置，并进行优化调整；

b.对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，启用路由器中的 ACL 配置，提高接入的安全性等措施优化配置，实现设备加固。

（3）安全设备加固

a.根据相关策略对设备进行检查与设置，并进行优化调整。

b.对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，提高接入的安全性等措施优化配置，实现设备加固。

4、在信息系统完成风险梳理和整改实施之后，供应商需要再次通过测评手段对信息系统的安全技术和安全管理上各个层面的安全控制进行整体性验证，提供的验收测评服务将协助本单位完成等级保护测评工作，对信息系统的安全等级保护情况及整改情况进行评审，完成区公安局备案，出具《网络安全等级保护等级测评报告》。

3.3 服务工具要求

1、漏洞扫描服务工具

本项目漏洞扫描服务需供应商自行准备漏洞扫描服务工具，为确保服务质量，所提供的漏洞扫描服务工具需具备以下能力：

▲服务商所采用的漏洞扫描设备或系统应在服务期内（2025 年 1 月 1 日-2025 年 12 月 31 日）具备质保能力，各种规则库应能保持更新，确保工具对于最新漏洞的识别能力（提供所用漏洞扫描设备或系统服务期间质保有效期截图或证明材料）

2、实施运维人员终端防护工具

为实现对运维实施人员运维电脑终端的安全管控、访问控制，供应商需自行提供一套终端安全防护工具，工具由后端统一安全管理平台和前端终端防护设备组成。工具需具备以下能力：

▲后端管理平台支持对前端防护设备进行统一管控，可实现统一管理、策略下发、行为监控；可实现终端网络行为日志存储、展现与分析。（提供截图证明）

▲支持在后端管理平台对前端防护设备采取执行或撤销软 Bypass 及硬 Bypass 操作，提高系统高可用性，当前端防护设备断电或故障时，被保护的运维终端网络访问不受影响。（提供截图证明）

▲支持学习指定被保护终端网络行为，可将学习结果转化为策略；支持以直接添加网络五元组、策略方向、指定安全防护设备的方式配置防护策略；支持验证策略执行情况，可查看指定网络五元组间已有策略情况。（提供截图或文件证明）

▲为避免前端防护设备被攻击破坏，无需为防护设备配置 IP 地址，前端防

护设备部署不改变现有网络架构；无需在被保护终端上安装任何软件代理；无IP的前端防护设备能够被管控平台统一纳管。（提供截图或文件证明）

▲可基于网络五元组的细粒度访问控制，可实现黑白灰三类名单过滤；可对风险行为进行识别、告警、阻拦，有效过滤非法访问，实现精准的运维终端安全防护。（提供截图或文件证明）

▲工具可支持对人员生物识别（如指纹）身份认证，落实接入院内网络运维人员身份不可否认性。（提供截图或文件证明）

4.人员要求

项目实施期间，指派1名工程师提供现场服务，实施过程中接受采购人安排管理，入场前签署保密协议，按采购人要求时间开展工作，工程师现场做好项目的跟进、协调、整改咨询、进度汇报等事宜，且每周提供项目工作周报。

（1）成交供应商须按其响应文件中承诺提供的项目组人员必须按要求投入到本项目中，在合同期内不得擅自更换。成交供应商如因工作安排或其他原因，需要更换项目组人员时，应事前向采购人书面提出书面申请，未经采购人同意，不得更换人员。

（2）如成交供应商未经采购人书面同意擅自更换项目组人员，除须按采购人的要求对人员作出调整外，累计达3次后，采购人有权终止合同，由此引致的经济损失，成交供应商须全额赔偿，采购人保留追究成交供应商相关责任的权利。

（3）采购人有权以书面形式要求成交供应商更换不能按规定履行合同的人员。

（4）即使是采购人要求或同意更换的人员，其代替人员的资质仍应得到采购人的认可，且其资历和经验均不低于被更换人员。由此而产生的费用由成交供应商承担。

（5）成交供应商对其投入的服务人员的人身安全负全部责任。

5.知识产权要求

本项目实施中所产生的所有工作成果（包括但不限于发明、发现及相关技术资料、文档等）的知识产权归广东医科大学顺德妇女儿童医院（佛山市顺德区妇幼保健院）所有。成交供应商保证所提供的服务没有侵害任何第三方的知识产权

或其他正当权益。如有第三方指控成交供应商提供给采购人的服务侵犯了该方的知识产权或其他权利，成交供应商应自费就上述指控为采购人辩护或进行妥善处理，并承担给采购人及第三方造成的一切损失（包括但不限于赔偿金、律师费等）。如成交供应商不为采购人辩护或不进行妥善处理，采购人可自行处理，采购人与第三方达成的和解协议或法院生效判决由采购人承担的责任，及采购人自行处理所支出的费用（包括但不限于律师费、案件受理费、执行费、差旅费等）由成交供应商承担。

6.保密要求

（1）在服务期间，成交供应商派驻服务团队须严格遵守采购人制定的各项规章制度、管理流程以及操作规范。如有违反，将追究服务商责任。

（2）不论何时（服务期间或服务期结束后），成交供应商须对安全服务过程中接触的采购人所有信息和数据保密。未经允许不得以任何方式向外界传递或泄露采购人的任何信息或数据，一旦发现，将追究成交供应商法律责任。

（3）对采购人的全部资产（包括全部设备、线路、软件、配套设施、系统产生的各类数据信息及相关文档资料等），成交供应商不得以任何方式对其进行出售、抵押或转移；且在服务期间，成交供应商有责任保证上述资产的完整、安全并处于良好状态，因成交供应商责任而导致的设备损坏或资产损失，由成交供应商承担责任。

7.培训

成交供应商需针对每个被测评的信息系统，为该系统的使用责任人提供1次线下培训，在培训过程中专业讲解对应的信息化系统在测评时发现的问题情况及提供整改和解决思路、措施和策略。

8.最终交付资料

包括但不限于：信息系统等保评测项目差距整改报告、信息系统等保测评报告、当地公安机关备案回执。

六、付款方式

签订后乙方出具等额发票，甲方在 30 个工作日内支付合同款 50%的预付款，甲方自收到当地公安机关出具的备案回执后，乙方应在甲方收到当地公安机关出具的备案回执起 10 个自然日内按最终采购款的 50%金额开具发票交给甲方，甲方收到发票之日起 30 个工作日内支付发票款。因乙方原因逾期交发票的，甲方付款天数相应顺延。

因甲方使用的为财政资金，甲方在前款规定的付款时间为向上级主管部门提出办理财政支付申请手续的时间（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为甲方已经按期支付。

七、验收标准

对本项目清单内系统逐一进行信息系统安全等级保护状况进行全面测评与综合评估，完成信息系统的年度测评。信息系统能通过 GB/T22239-2019 等级保护 2.0 的国家标准，出具等保测评报告等资料并成功在当地公安机关备案代表通过验收。

八、评选标准

评分内容	技术部分	商务部分	价格部分
权重	40%	30%	30%

序号	评审项目	评分标准	分值
技术部分（总计 40 分）			
1	实施计划及实施方案	投标人针对本项目拟写实施计划及实施方案，包括但不限于实施计划详细描述实施计划（包括各阶段重点任务、时间节点、人员安排等）及实施方案（技术要点、解决思路、建设规划等）： 1、实施计划详细描述实施计划及实施方案完整、全面，技术路线清晰，科学合理，可操作性强，得 12 分； 2、实施计划详细描述实施计划及实施方案较完整、较全面，技术路线较清晰，较科学、较合理，可操作性较强，得 8 分； 3、实施计划详细描述实施计划及实施方案基本完整、基本全面，技术路线基本清晰，基本科学、基本合理，有一定可操作性，得 4 分； 4、实施计划详细描述实施计划及实施方案不够完整、	12

		不够全面，技术路线不够清晰，不科学、不够合理或无提供的，得 0 分。	
2	技术服务团队能力	拟委派的项目经理必须具有计算机相关专业本科或以上学历，同时具备： 具有项目管理专业人员资格认证（PMP 认证）； 满足得 3 分，其他不得分； 拟委派的项目现场负责人（与本项目经理不为同一人）具有本科或以上学历，具备： （1）具有中国信息安全测评中心颁发的 CISP 证书； （2）具有高级信息系统项目管理师认证证书； （3）具有 Oracle 数据库原厂 OCP 认证证书； （4）具有人社局颁发的网络工程师中级或以上认证证书。 （5）具有容灾实施专家认证； 上述条件每满足 1 项得 3 分，最高得 15 分。 注:投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前连续六个月内任一个月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。	18
4	技术要求响应程度	1.响应内容全部满足需求书中重要技术参数（打“▲”号条款）的，得 8 分；每负偏离一条扣 1 分（本需求共有 8 条重要技术参数）。 2.技术参数的响应内容全部满足用户需求书中一般技术参数（打“★”号条款）的，得 2 分；每负偏离一项扣 1 分（本需求共有 2 条一般技术参数）。	10
商务部分（共计 30 分）			
5	投标人管理体系资质要求	具有较完备的管理体系，投标人具有有效的： （1）具有《信息安全管理体系认证证书》，得 2 分； （2）具有《质量管理体系认证证书》，得 2 分； （3）具有《环境管理体系认证证书》，得 2 分； （4）具有《IT 服务管理体系认证》，得 2 分。 注：需提供证书复印件和全国认证认可信息公共服务平台上该证书的查询结果截图并加盖投标人公章，否则不得分。	8
6	投标人服务能力	1、具有 ITSS 数据中心服务能力成熟度标准符合性证书二级和具有 ITSS 信息技术服务运行维护服务能力成熟度模型，满足得 2 分，不满足不得分； 2、具有信息系统建设和服务能力等级证书满足得 2 分，不满足不得分； 3、具有中国网络安全审查技术与认证中心 CCRC 颁发的信息安全服务资质-认证方向为信息系统安全集成、安全运维服务、信息安全风险评估证书。每个得 2 分，满足得 6 分；	12

		4、具有计算机信息系统安全服务等级证书，满足得 2 分，不满足不得分；	
7	相关项目经验	投标人 2020 年 1 月 1 日至今在同类等保测评服务项目实施经验，每个 2 分，最高 6 分； 注：须提供合同关键页（至少含合同首页、项目名称及内容页、签字盖章页）和发票并加盖投标人公章，同一合同不可重复得分，有效时间以合同签订时间为准。	6
8	培训方案	技术培训方案的完整性与针对性，根据投标人提交的培训方案进行评分。 (1) 培训方案内容全面且方案设计科学合理、可操作性强、针对性强，得 4 分； (2) 培训方案内容较为全面且方案设计较为科学合理、基本具备可行性，存在改善空间的，得 2 分； (3) 培训方案内容缺失较多且方案设计不够科学，得 1 分。 (4) 未提供相关培训方案，不得分。	4
价格部分（总计 30 分）			
1	评选标准	经评选小组审核，满足采购文件要求，以折扣率最低者定为评选基准价，其对应报价得分为满分。	30
2	计算公式	报价得分＝（评选基准价÷评选最后报价）×价格分值	