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）网络安全服务项目需求书

一、项目范围：

本次网络安全服务针对医院信息系统整体安全的现状，提供专业化安全管理和服务，项目范围涉及到以下内容:

1、医院安全设备，包括边界类设备、摆渡类设备、旁路设备等；

医院现有运行系统的后台支撑系统（如操作系统、数据库）相关安全配置和服务，如系统安全补丁通知、操作系统端口防护等；

2、管理体系认证：

（1）具有 ISO9001 质量管理体系认证；
（2）具有 ISO27001 信息安全管理体系认证；

3、安全服务能力认证：

（1）中国信息安全测评中心认证的注册信息安全工程师

（2）网络工程师具有 CCRC CISP 证书、网络工程师或者以上认证

（3）具备广东三甲医院安全服务案例不少于 3 个

二、项目预算：

序号	采购内容	项目预算	项目期限
1	网络安全服务项目	12 万元	1 年

三、具体需求内容：

1、定期安全检查

服务频次：每季度一次

服务内容：对医院的现网整体安全提供全面的巡检服务，巡检的内容包括但不限于：

(1) 安全设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备标签完善程度；

(2) 安全设备软件版本信息、当前 IOS 版本信息、最新 IOS 版本信息、设备持续运行时间、设备 IOS 备份情况、设备 CPU 利用率、设备内存利用率、设备模块运行状态、设备风扇及电源状况、设备端口数量、设备端口类别、设备端口类型、设备运行机箱温度；

(3) 安全设备连通性、冗余协议运行状态、VLAN 信息、以太通道信息、路由协议、邻居关系、交换协议、生成树 STP 协议、NAT 连接数状态、FLASH 信息、设备配置信息分析、多余配

置信息分析、配置精简建议、IOS 安全建议、防火墙信息、防火墙策略、防火墙 DMZ 区检查、防火墙 Xlate 状态、应用业务、IP 地址使用状况；

(4) 对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估；

(5) 对安全系统瓶颈和资源竞争情况进行分析，找出潜在问题。

(6) 对服务器、终端做周期检查，主要内容是检查是否存在高危漏洞，杀毒软件病毒库是否最新。如果发现问题需要及时提供人工现场处理修复或者升级服务。

2、安全配置备份

服务频次：不定期备份，一个季度至少一次

服务内容：

(1) 为了保证安全设备的健康运行情况，使得设备在失效或配置丢失时，能依靠备份尽快地恢复系统与配置，保护关键策略，保证配置不丢失，特制定本服务。

(2) 关键的网络安全设备的策略配置进行备份，防止策略的丢失与错误变更配置；涉及备份和恢复的事由专人负责备份工作，并认真填写备份日志。

(3) 备份数据应该严格管理，妥善保存；备份资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

(4) 一旦发生配置丢失或数据破坏等情况，要由负责人员进行备份数据的恢复，以免造成不必要的麻烦或更大的损失。

3、安全风险评估

半年一次，在现网架构改动、新系统上线、配置变更的时候，对变动带来的风险进行识别和评估，提出风险预防和必要的整改措施。

4、安全设备配置适应性调整

服务频次：一年内不限次数

服务内容：在安全相关设备配置需要调整时，如：安全策略调整、新链路配置、产品参数调整等；派遣工程师进行配置风险评估、提出调整方案并实施。安全相关设备配置包括但不限于以下情况：

(1) 网络出口新增加，评估新网络出口的风险和安全防护措施；

(2) 防火墙、UTM 等边界类设备的配置变更，详细记录变更内容，包括 IP 策略、端口策略、放通/禁止策略等；

(3) 网闸等隔离类设备的配置变更，详细记录变更内容，包括 IP 策略、端口策略、应用通道、转发模式等；

(4) 入侵防御、网络行为分析等旁路安全设备配置变更，包括协议监控、端口监控、联动策略等；

(5) 杀毒软件、准入控制等终端管理类软件的配置变更，包括扫描策略、准入方式、控制范围等；

(6) 协助医院进行安全设备或软件的配置变更时，要充分考虑到配置变更过程中和变更后带来的安全风险，采取一定的预防措施，将风险降低到最小，最小化对医院正常业务开展的带来的影响。安全事件紧急响应：一年内不限次数，在出现安全事故、数据泄密、网络入侵

等安全事件的时候，紧急响应，快速定位和查找问题，制定出解决方案，第一时间把安全问题消灭在萌芽状态。

5、安全事件紧急响应

服务频次：一年内不限次数

服务内容：在接到医院的安全事件紧急救援服务请求后，本地安全工程师立即响应，通过预先确认的远程连接方式登录到相应的系统上，对安全事件进行排查，在发现远程登录无法解决的安全事件后，立即采用最快的交通方式赶赴甲方现场，2 小时内可达到医院的现场。如信息系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、黑客攻击、蠕虫或大面积爆发病毒等，常驻广州的安全团队将在 2 小时之内赶赴现场协助解决问题，必要时应提供入侵调查分析、安全审计预警与黑客追踪服务。

应急响应服务包括远程应急响应服务和本地应急响应服务，其主要内容如下：

(1) 消除潜在安全隐患： 通过日志信息和其他必要信息，检查后门程序和网络系统漏洞，消除其再次受到攻击的可能性，即消除今后的安全隐患，对系统的安全进行重新评估。

(2) 检查安全日志： 通过检查系统、防火墙、路由器等系统安全日志，为确认攻击来源和攻击手段以及调查取证提供必要的条件。

(3) 入侵者追踪： 通过所能得到的信息追踪入侵者，并记录其尽可能多的信息，为调查取证提供条件。

(4) 主机恢复： 在甲方信息系统网络或主机受到攻击并且出现网页遭替换或系统丢失等恶性事件后，确认已经消除安全隐患，在系统网络管理人员的协助下，对应用系统或操作系统进行恢复，保证系统资源在第一时间内的可使用性。

(5) 网络恢复： 医院信息系统的核心交换机、路由设备等网络设备出现问题，在确定是受到攻击所造成的情况下，确认已消除安全隐患，在经过医院授权后，对网络设备进行恢复，保证医院信息系统网络资源在第一时间内的可使用性。

6、安全建设配合响应

服务频次：一年内不限次数

服务内容：在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全技术人员指导配合进行安全相关工作，工作内容包括但不限于以下内容：

(1) 医院网站漏洞排查；

(2) 公安部门递送的安全检查或安全漏洞通知；

(3) 上级部门递送的安全检查或安全漏洞通知；

(4) 国家重大节假日的安全保障检查；

(5) 突发性事件的检查通知或现场检查；

(6) 护网安全保障检查

(7) 等级保护评审配合工作。

在上述事件发生的时候，医院需要有安全水平高的行业技术人员配合医院开展安全方面相关工作，根据约定的时间安排专业安全工程师提供远程或上门的安全相关服务，具体服务内容由医院根据具体要求商议决定。

7、系统漏洞扫描与分析

服务频次：每季度一次

服务内容：定期利用专业的技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、网站漏洞扫描、数据库漏洞扫描等，扫描相关使用的专业工具版本由乙方提供，医院无需为该工具支持额外费用。

对服务器主机、业务终端设备发现的问题或安全漏洞提出整改建议，并协助甲方做好整改工作。包括服务器高危漏洞在不影响业务的情况下协商修复；终端健康情况检查。系统加固服务：一年约 10 个服务器 IP，根据专业安全检测结果，制定相应的系统加固方案，针对不同目标系统，通过安装补丁、修改安全配置、增加安全机制等方法，合理的进行安全性加固。

8、系统加固服务

服务频次：一年约 10 个服务器 IP

服务内容：根据专业安全检测结果，制定相应的系统加固方案，针对不同目标系统，通过安装补丁、修改安全配置、增加安全机制等方法，合理的进行安全性加固。

9、安全培训服务

服务频次：一年两次

服务内容：配合医院展开安全建设和运维的工作，定期对医院信息科相关人员提供信息安全技术培训，培训结束后定期进行技术考核，提升医院信息安全意识和技术知识水平。

培训对象：医院系统管理员、网络管理员、数据库管理员、安全审计员等专业技术人员。

培训内容包括但不限于以下内容：

(1) 国家等级保护流程与相关内容

(2) 医疗行业等级保护建设案例分享

(3) 医疗行业内外网互联安全建设风险

(4) 医疗行业网站建设和漏洞防范介绍

(5) 医疗行业数据库安全和漏洞防范介绍等。

10、主机基线检查

服务频次：一年约 10 个核心业务服务器 IP

服务内容：根据相关法律法规、行业标准制定用户安全基线基准。

安全配置检查内容：系统管理和维护的正常配置，合理配置，及优化配置。配置检查主要针对操作系统、网络设备、安全设备、数据库等，检查项包括系统目录权限，帐号管理策略，文件系统配置，进程通信管理等方面，例如日志及审计、备份与恢复，加密与通信，特殊授权及访问控制等安全特性。

四、参考评分：

评分比重如下：

评分内容	技术部分	商务部分	价格部分
权重	50%	25%	25%

1.技术评价：

序号	评审内容	分值	评分细则
1	对用户需求书中服务要求内容的符合性	20	所投服务内容全部满足用户需求书中对服务的要求，得 20 分； 每出现一处负偏离，扣 2 分，扣完为止。
2	项目维护方案比较	8	项目整体服务方案，项目服务质量保证方案（服务方式、流程等），项目实施方案，对具体方案设计进行综合评审。服务方案具有前瞻性、合理性、可靠性、可扩展性和全面性，提供的服务质量保证及实施方案满足项目实际需求且具体详尽的得 8-7 分；服务方案前瞻性、合理性、可靠性、可扩展性一般，提供的服务质量保证及实施方案符合项目需求的得 6-4 分；提供服务方案、服务质量保证及实施方案较为简单的得 3-1 分；无提供得 0 分。
3	应急响应流程和应急响应规划合理性	6	响应内容完整、详细、表述清晰、科学合理，得 5 分；响应内容比较完整、详细、表述清晰、比较合理，得 4-3 分；响应内容基本完整、详细、表述基本清晰、合理，得 1 分；响应内容不完整、不够详细、不清晰、可行性差，得 0 分。
4	本项目经理的资质，提供项目经理在本公司任职的外部证明材料	8	具有以下证书（在有效期内），须提供证书复印件： ① 全日制本科或以上学历且工作经验不少于10年（以毕业证的时间计算）； ② 项目经理本人有高级信息系统项目管理师证书； ③ PMP 认证证书； ④ 具有 RHCH 认证； ⑤ 中国网络安全审查技术与认证中心认证的风险管理专业级或以上证书； ⑥ 容灾实施专家认证； ⑦ IT 服务工程师认证。 以上完全满足得8分，一项不满足扣2分，扣完为止。 注：须提供学历、资质证明材料及项目经理在投标人服务的外部证明材料扫描件，如投标截止日之前六个月以内任意月份的代缴个税税单或参加社会保险的《投保单》或《社会保险参保人员证明》等。无提供的不得分。
5	技术服务团队能力认证情况	8	本项目服务人员通过以下认证：

			1）具有 OCP 工程师认证的每个得1分，最高2分； 2）本项目服务人员通过中国信息安全测评中心认证的注册信息安全工程师，每个得1分，最高2分； 3）技术团队通过中国网络安全审查技术与认证中心颁发的风险管理专业认证，每个得1分，最高2分； 4）技术团队通过中国网络安全审查技术与认证中心颁发的应急服务专业认证，每个得1分，最高2分； （需提供人员的相关证书复印件加盖公章和近三个月的社保证明材料，同一个人不同资质可重复计分。）

2.商务评价：

序号	评审内容	分值	评分细则
1	投标人资质情况	9	投标人具有以下有效： 1) ISO9001 质量管理体系认证； 2) ISO/IEC 20000 IT 服务管理体系认证； 3) ISO 27000 信息安全服务管理体系认证； 4) ISO14001 环境管理体系认证； 5) 有信息系统建设和服务能力认证； 6) 知识产权管理体系认证； 完全满足得 9 分，有一项不满足扣 2 分，扣完为止。 （提供证书复印件加盖公章，原件备查）（提供有效的证书复印件加盖公章，原件备查）
2	投标人荣誉及服务能力	6	1、投标人具有计算机信息系统安全服务等级证认证得 2 分，不满足不得分； 2、投标人具有高新技术企业证书证书得 2 分； 3、投标人具有安全相关的软件著作权证书（如安全运维系统、安全加固系统等），每一个得 1 分，最高得 2 分； （提供有效的证明材料复印件加盖公章，原件备查）
3	技术服务团队情况	2	投标人应在广东省内设有固定的售后服务场所和稳定的技术服务团队，团队≥30 人的得 2 分。售后服务场所和技术服务团队均应提供营业执照和参保证明的证明材料，不提供证明材料不得分。
4	投标人的实施经验情况	8	投标人自 2020 年 1 月 1 日至今签定的广东省内医疗行业有安全维护服务的实施经验，每个 2 分，最高 8 分。 （提供有效的合同复印件加盖公章）

3.价格评价：

评审项目	分值	评分细则
价格	25	价格分是以满足招标文件要求且投标价格最低的投标报价为评标基准价，其他投标人的价格分则按比例算出。 价格分＝（评标基准价/投标报价）×25