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：2023年网络安全服务项目

2023年 8月

一、采购项目情况概述

我院已在前期的信息化项目中分别对基础硬件配套设施、安全防护建设和应用系统升级改造进行了部分改造，已基本完成了网络安全建设，本次引进网络安全服务项目，通过第三方安全服务加强院内系统及设备安全管理功能，有效运用院内相关的安全设施，确保设施设备被充分利用起来。

二、项目采购内容

1. 项目清单

序号	项目名称	数量	单价（元）	预算总金额（元）	服务期
1	网络安全服务项目	1	260000	260000	一年
合计：（单位人民币元）				260000	
备注：					

三、项目实施地点：

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）指定任何服务地点。

四、项目预算金额：

合计不超过 260000 元人民币。预算中包括但不限于服务费用、人力费用以及完成本项目内容所需的一切费用等。

五、项目要求

1.资质要求

（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）具备 CCRC 信息系统安全运维认证、信息系统安全集成；

2.服务要求：

➢ 本项目将计划在顺德妇幼开展相关安全服务，具体服务内容如下：

序号	具体内容
1	**定期安全检查：**每季度一次，分析现网的安全风险，发现潜在的系统漏洞，排查网络中潜伏的未知风险和威胁。
2	**安全设备配置备份：**不定期备份，一个季度至少一次，建立安全设

	备台账。通过配置备份，保障设备运行健康，以防出现变更导致的错误，提高应急处置能力。
3	**安全设备配置适应性调整：**一年内不限次数，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；乙方必须派遣工程师进行配置风险评估、提出调整方案并实施。
4	**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	**安全建设配合响应：**一年内不限次数，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，派遣专业安全专家指导配合进行安全相关工作。
6	**漏洞扫描：**每季度一次，使用系统漏洞扫描工具对 数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认，提出整改建议。
7	**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	**安全培训：**一年内两次，安全攻防技术培训，全单位信息安全意识培训，单位网络安全意识宣传等。
9	**主机基线核查：**一年核心服务器 IP 配置，保障系统最基本的安全要求。
10	**安全管理制度梳理：**根据客户的各类管理内容建立安全管理制度，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。
11	**资产梳理：**终端科室检查准入控制信息的登记情况，对所有合法进入网络的计算机在入网前将进行必要的安全检查，确保每台计算机都符合既定的安全规范

12	**渗透测试：**一年两次，每次不超过 5 个系统。渗透测试通过模拟黑客思维及行动模式，使用主流的攻击技术对目标网络、系统、数据库进行模拟攻击测试,提前发现系统潜在的各种高危漏洞。
13	**应急演练：**每年一次，根据突发网络安全事件的性质，深度切合医院所面临的实际网络安全问题。为医院提供分门别类的演练方案；突发网络安全事件演练解决方案应急演练场景可分为：有害程序事件演练，网络攻击事件演练，信息破坏事件演练，设备实施故障演练和灾害性事件演练。
14	**重保值守：**安全监控：WAF、防火墙、态势感知、杀毒软件；攻击 IP 封禁、威胁主机断网隔离、日志溯源

- 详细服务要求如下：

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。

4.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，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，安全团队需在 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。

5.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。

6.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。

7.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。

8.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。

9.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。

10.安全管理制度梳理

服务内容：在安全策略方面，依据国家信息安全战略的方针政策、法律法规、制度，按照等级保护相关标准规范要求及各监管机构对上市公司的内控要求，结合科技公司自身的安全环境，制订完善的信息安全策略体系文件。信息安全策略体系文件应覆盖信息安全工作的各个方面，对管理、技术、运维体系中的各种安

全控制措施和机制的部署提出目标和原则。

11.资产梳理

服务内容：安全服务团队结合资产梳理工具成果进行梳理，识别出网站资产、服务器资产、终端资产，并形成资产清单。

第一次资产梳理：安全服务团队使用安全运营平台进行资产发现，并导入已知资产信息，形成初步资产表。

日常资产梳理：安全服务团队对运营平台自动发现的未知资产进行确认，指定资产责任人并为其分配用户。

12.渗透测试

服务频次：一年 2 次，每次不超过 5 个业务系统。

服务内容：渗透测试主要是模拟黑客的攻击方法，检测网站、网络协议、网络服务、网络设备、应用系统等各种信息资产所存在的安全隐患和漏洞。

渗透测试主要分为扫描和人工两部分，依靠带有安全漏洞知识库的网络安全扫描工具以及安全专家对漏洞的深入了解，其特点是能对被评估目标进行覆盖面广泛而且更深度的安全漏洞查找，并且评估环境与被评估对象在线运行的环境完全一致，较真实地反映网站及服务器系统、网络设备、应用系统所存在的安全问题和面临的安全威胁。

13.应急演练

服务频次：一年 1 次。

服务内容：根据应急演练规划和应急预案要求，在对事先设定事件场景风险和应急预案认真分析的基础上，结合年度内发生网络安全事件的情况，发现存在的问题和薄弱环节，确定需洞整的演练人员、需锻炼的技能、需检验的设备、需完善的应急处萱流程、指挥词度程序以及需进一步明确的职责等，分析完成举办应急演练的要求。

14.重保值守

服务内容：在攻防演习实战期间，安全监控小组将对外部安全威胁情报、安

全漏洞情报及外部披露情报等安全情报进行实时监控，通过对医院内部安全设备进行监控预警，日志分析，实时从设备告警日志中捕获异常攻击行为或操作行为，通过策略调优、误拦分析，及时封堵异常攻击行为，对安全风险进行闭环等。

六、付款方式：

按合同约定付款方式进行支付。

七、验收标准：

验收标准：每项服务完成后，应在用户规定的时间内（3-5 个工作日）出具相应服务报告，服务报告将作为项目最终验收主要依据。

八、其他

出现下列情形之一的，本项目合同终止：

（1）本项目顺利完成。

（2）在本合同服务期内，因不可抗力的情形导致本合同无法继续履行的，而由此导致毁损并造成的损失双方互不承担责任。

（3）经双方协商一致解除本项目合同的。

（4）配合采购人和需求科室完成合同签订等工作。

（5）其他未尽事项另行商谈确定。

九、评选参考标准

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	评分细则及标准	分值
技术部分（总计 40 分）			
1	投标人的项目经理资质要求	1、具有信息系统项目管理师认证证书； 2、具有 Oracle 数据库原厂 OCP 认证证书； 3、具有项目管理专业人员资格认证（PMP 认证）； 4、具有 RHCE 认证证书； 5、具有 HCIP 认证证书； 6、具有信息安全保障人员认证证书； 7、具有容灾实施专家认证； 8、具有 ITSS IT 服务工程师证书； 项目经理具备以上有效期内的资质证书，每个证书得 1.5 分，共 12 分。	12

		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六个月内《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。	
2	投标人技术服务团队能力	1、服务团队中有 OCP 数据库工程师认证，每个得 0.5 分，最高得 2 分； 2、服务团队中有人社局颁发的网络工程师中级认证每个得 0.5 分，最高 2 分； 3、服务团队有 VMware 认证（VCAP），每个得 0.5 分，最高得 1 分； 4、服务团队有信息系统项目管理师认证（除项目经理外），每个得 0.5 分，最高 1 分； 5、服务团队有系统架构设计师，每个得 1 分，最高 1 分； 6、服务团队有注册信息安全专业人员，每个得 0.5 分，最高 3 分； 7、服务团队有 RHCE 认证证书，每个得 0.5 分，最高 2 分； 8、服务团队有 HCIE 认证证书，每个得 0.5 分，最高 1 分； 9、服务团队有 ITIL 认证证书，每个得 1 分，最高 2 分； 注:一人有多证，只算一种认证得分；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六个月内的《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。	15
3	项目管理方案及质量保障措施	根据投标人对针对本项目的服务方案、保障措施是否完整，详细、可行、有效，具有可操作性及技术性能指标的成熟性、稳定性、先进性以及关键重要部位控制措施是否明确、详尽、合理作为评审依据。 优：投标人的服务方案具有完整的保障措施，并且详细、可行、有效，具有可操作性的得 10 分； 良：投标人的服务方案具有一定的保障措施，并且具有一定的可行性、有效性、操作性的得 5 分； 中：投标人的服务方案具有不完善的保障措施，具有一些可行性、有效性、操作性的得 3 分； 差：投标人的服务方案具有不完善的保障措施，不具有可行性、有效性、操作性的得 1 分； 无服务方案不得分	10
4	本地服务情况	投标人在项目所在城市有固定的服务场所和售后服务团队（提供营业执照（产权证明或租赁合同）和本地购买社保的证明）； 提供证明文件得 3 分，不提供不得分	3
商务部分（总计 30 分）			
6	投标人管理体系	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、具有 ISO14001 环境管理体系认证； 4、具有 ISO20000 IT 服务管理体系认证； 5、具有知识产权管理体系认证证书； 投标人具有上述 5 项认证，一个认证得 2 分，满分得 10 分； 注：1.提供与投标人名称一致的有效的相关质量认证证明文件复印件，并加盖投标人公章；2.上述证书的发证机构须为境内机构；否则不得分。）	10

7	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满足得 1 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 CMMI 能力成熟度模型证书，满足得 2 分，不满足不得分； 4、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 1 分，满分 3 分； 5、具有高新技术企业证书，满足得 1 分，不满足不得分； 6、具有计算机信息系统安全服务等级证书，满足得 1 分，不满足不得分； 7、具有数据库安全相关的软件著作权，每具有一个得 0.5 分，最高 2 分；	12
8	类似项目经验	投标人自 2020 年以来在广东省内有三甲医院安全服务实施经验，每个 2 分，最高得 8 分。（提供合同复印件作为评审依据，否则有可能影响评审结果）。	8

价格部分（权重 30%）

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。

报价得分＝（评选基准价÷评选最后报价）×价格分值