**惠州市中大惠亚医院网络安全服务项目技术要求**

**用户需求**

1. **项目概况**

本项目为我院网络安全系统运维保障服务项目，主要用于保障医院网络安全设备的稳定运行。按照国家、省等发来的《关于印送<贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见>的函》（公网安[2020]1960号）和《广东省卫生健康委办公室关于加强网络与信息安全工作的通知》）（粤卫办函〔2019〕285 号）等系列文件要求，各单位应加强网络与信息安全日常管理工作和日常防护。目前医院原网络安全系统维保服务于2023年9月7日合同到期，亟需对医院网络安全系统的安全防护特征库和安全运维服务进行下一年度的延续维保，提升医院整体的安全防护能力，保障医院信息系统的稳定安全运行。

1. **项目总体要求**

为了更好的维护医院网络及信息系统的安全稳定，结合我院信息系统多、网络结构复杂、安全运维人手不足等实际情况，按医院信息化建设工作安排拟开展我院网络安全服务项目工作，对现有防火墙、入侵防御、数据库审计、IDS、日志服务器、防病毒等网络安全设施进行特征库升级，并提供专业安全技术支撑服务对我院网络安全状况进行梳理和风险排查，对安全设备进行统一管理运维，对安全服务过程中发现的风险点和系统漏洞提出科学、可行的修复加固计划和建议，建立符合国家标准的安全管理体系，达到保障医院网络及信息系统的安全稳定运行的目的。

1. **项目服务内容**

**1、服务范围**

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技术服务，服务范围涉及到以下内容：

（1）医院核心网络，包括医院内网和外网的设备与环境运维；

（2）医院现有安全设备，包括边界类设备、摆渡类设备、终端设备、旁路设备等设备与环境运维；

（3）配合医院完成医院网络安全管理制度的建设和运维；

（4）配合完成医院信息安全等级保护工作相关整改需求，整改设备另行采购；

（5）对现有安全设备：防火墙(AF)、上网行为管理、VPN、入侵防御、堡垒机、日志审计系统、网闸、入侵检测、数据库审计、态势感知、企业版杀毒软件、终端准入控制系统等设施的维保和特征库升级，并结合医院管理需要，参照等保分级保护相应标准实施差距分析和整合运维管理；

（6）结合网络安全等级保护及医院管理需要，对主机安全（包括但不限于服务器、终端、其他计算机设备等）、系统安全（包括但不限于windows、linex等）进行配置核查，网络安全巡检、网络安全风险处理等系列维护服务。

(7）本次信息安全服务驻点运维服务期为壹年。

**2、项目服务清单**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务项目** | **服务内容简述** |
| **一、安全设备部分** |
| 1 | 下一代防火墙升级维保服务 | 产品维修服务，包含系统软件版本升级服务，IPS漏洞防护、服务器防护功能模块更新，特征库升级服务，一年期 |
| 2 | 上网行为管理升级维保服务 | 产品维修服务，包含系统软件版本升级服务，URL&应用识别规则库升级维保服务，一年期 |
| 3 | VPN维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期 |
| 4 | 网闸维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期 |
| 5 | 堡垒机维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期，200用户授权 |
| 6 | 入侵检测系统（IDS）维保服务 | 产品维修服务，包含系统软件版本升级服务，特征库升级授权，一年期 |
| 7 | 态势感知系统维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期 |
| 8 | 日志审计系统维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期 |
| 9 | 数据库审计系统维保服务 | 产品维修服务，包含系统软件版本升级服务，一年期 |
| 10 | 终端安全管理系统升级维保 | PC端防病毒功能、补丁管理升级维保服务。包含一年更新服务，一年期，终端数700 |
| 服务器终端功能、补丁管理升级维保服务。包含一年更新服务，一年期，终端数60 |
| 支持外设管理、进程管理、违规外联、能耗管理、网络管控等。支持主流Windows PC客户端操作系统，包含一年更新服务，一年期，终端数700 |
| **二、安全运维服务部分** |
| 1 | 安全巡检与安全加固 | 通过对医院重要的服务器、网络、安全设备、操作系统等例行巡检，发现并提供安全加固和配置优化建议。对中间件、安全设备、网络设备等进行安全配置加固和网络架构安全调优，针对不同设备和系统提供相应的安全加固方案，并协助院方进行安全加固，记录加固条目和结果。 |
| 2 | 安全风险评估 | 风险评估服务是指参照GB/T 31509-2015等信息安全风险评估实施指南以及国家信息安全等级保护等安全标准进行资产梳理和风险评估的工作，针对医院资产重要程度分别提供不同频率和方式的安全评估，帮助医院了解客观真实的自身网络系统安全现状，以及医院当前信息系统面临的安全风险，并为医院提供风险规避建议及根据医院需求提供整改方案。 |
| 3 | 应急响应服务 | 当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助医院快速止损，最大化降低安全事件带来的影响 |
| 4 | 安全设备日志分析 | 从安全设备各结点获得日志文件，采取人工+工具的分析分析方法，形成日志分析报告。该报告与定期评估结果、定期策略分析结果进行综合分析，找到当前的系统及网络设备中存在的问题和隐患，并给客户提供专业的增强建议。 |
| 5 | 等保咨询服务 | 在测评机构实施等保测评期间，协助医院收集资料，配合整改配置策略，提供整改顾问建议，帮助医院顺利通过等保测评。 |
| 6 | 系统漏洞修复 | 每季度一次，在通过安全检查、漏洞扫描等方式发现操作系统、数据库、中间件等通用软件的潜在高危安全漏洞时，配合医院维护人员进行系统漏洞修复工作，该工作需要评估修复带来的潜在风险和保障修复后系统正常稳定运行。 |
| 7 | 制度完善服务 | 遵从等级保护2.0、ISO27000的合规要求及网信、卫健局等监管单位相关要求，完善目前缺失政策，并协助完成政策变动所需的管理制度的梳理及补充工作；协助建立医院本身的管理体系，输出《新增管理制度》 |
| 8 | 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；须派遣工程师进行配置风险评估、提出调整方案并实施。 |
| 9 | 网络安全规划 | 根据维护期间发现的安全隐患与运维工作成果，为医院进行全院网络安全建设规划与安全整改建议。 |
| 10 | 安全培训 | 为增强医院人员的安全意识、提升全员的网络及信息安全知识，通过当前典型的安全事件导入，定期开展信息安全宣传活动，宣传内容包括：网络及信息安全法律法规、员工安全意识、网络及信息安全制度等。 |

**3.技术服务具体要求**

## 3.1现有安全设备整合运维

1）对现有安全设备设施进行维保工作，并对特征库进行升级，保证各个安全设备特征库为最新版本，如出现设备硬件故障，在无法恢复其使用情况下，立即提供相同或优于故障设备功能和型号的设备予以替换，并提供采购清单对应厂家服务承诺函。

2） 结合医院业务管理需要，参照等保分级保护相应标准对医院现有安全设备和安全边界进行梳理，提出具有可操作性的建设方案，并完成各个安全设备协同整合管理。

3）涉及安全设备主要有：H3C防火墙、下一代防火墙、上网行为管理、VPN、入侵防御、堡垒机、日志审计系统、网闸、入侵检测、数据库审计、态势感知、企业版杀毒软件、终端管理等系统。具体内容详见上文“项目服务清单中技防设备部分”

**产生文档：**安全设备部署实施情况报告、安全设备资产清单

**服务频率：**按需

## 3.2 安全巡检与加固

通过对医院重要的服务器、网络、安全设备、操作系统等例行巡检，发现并提供安全加固和配置优化建议。对中间件、安全设备、网络设备等进行安全配置加固和网络架构安全调优，针对不同设备和系统提供相应的安全加固方案，并协助院方进行安全加固，记录加固条目和结果。

1）根据等级保护要求、安全服务人员的理解、业务的安全要求的结果等对网络层开展安全巡检工作。

2）网络架构巡检内容：网络架构脆弱性、访问控制、网络边界脆弱性、安全设备部署、日志管理、线路冗余、无线安全等。

3）网络安全设备巡检内容：认证授权、安全审计、运行维护、安全策略、接入位置及部署方式、自身安全性配置等。

4）安全加固：对巡检中发现的风险提供加固方案，并指导和协助院方进行加固操作。对重点服务器的操作系统和应用服务进行适度安全配置加固以及系统安全优化。

**产生文档：**网络信息安全巡检及加固报告

**服务频率：**至少4次/年

## 3.3 安全风险评估

风险评估服务是指参照GB/T 31509-2015等信息安全风险评估实施指南以及国家信息安全等级保护等安全标准进行资产梳理和风险评估的工作，针对医院资产重要程度分别提供不同频率和方式的安全评估，帮助医院了解客观真实的自身网络系统安全现状，以及医院当前信息系统面临的安全风险，并为医院提供风险规避建议及根据医院需求提供整改方案。

1）信息资产安全需求评估

帮助医院识别和统计信息系统关键资产，并参照CIA属性对各资产的机密性、完整性、可用性进行需求分析，帮助医院制定各资产的安全防护等级，提供相应承诺函。

2）物理环境安全评估

参照机房环境安全建设的有关国家及行业标准，评估现有机房环境的安全状况，指导未来机房安全改造建设。

3）网络架构和设备安全评估

评估网络架构设计的合理性和安全性，包括安全域划分、VLAN控制、路由设计、网络访问控制、安全审计措施等，对于网络架构中可能存在的各种安全隐患给出相应的安全改造技术建议；利用专业的漏洞扫描工具对网络中的关键网络设备进行安全分析，发现网络设备中存在的系统漏洞和配置安全隐患。

4）服务器漏洞检测

利用人工挖掘和专业的漏洞扫描工具对目标所有服务器系统进行全面的系统脆弱性检测，并对扫描结果进行人工分析；检查对象包括操作系统、应用服务平台、后台数据库等。

5）服务器人工审计

结合专家经验，参照国内国际权威安全审计CheckList，对重点服务器系统进行人工控制台审计评估，评估内容包括：用户账号及口令健壮性、系统安全配置、补丁更新情况、日志审核策略、受入侵迹象、可疑后门及木马清除等。

6） 应用系统安全评估

对于C/S和B/S结构开发的业务软件进行深层次的安全分析，主要针对系统的安全抗攻击能力，信息保密性与设计开发过程中的安全问题进行深度挖掘。

7） 关键数据安全保障评估

分析和评估关键数据在产生、传递、使用、存储、备份等过程中的安全保障措施，对于可能导致关键数据损失的严重隐患，我方将提供有针对性的合理建议。

8） PC终端安全性检测

利用多种专业漏洞扫描工具对关键网络区域的PC终端进行全面的系统脆弱性检测评估，并对扫描结果进行人工分析；检查内容包括补丁更新情况、账号弱口令、违规应用服务等。

9） 安全管理状况评估

参照国家（主要指等级保护）及行业相关政策要求以及国内国际权威的信息安全管理体系标准，采用访谈、问卷调查、文档审计等多种方式评估医院在信息安全管理方面的现状情况，包括：安全保障组织机构及人员配备情况、安全运维管理制度及流程、应急保障体系建设等，并提供相应的改善建议。

**产生文档：**风险评估分析报告和整改建议

**服务频率：** 1次/年

## 3.4 应急响应服务

当医院信息系统发生安全事件时，快速及时的为医院提供全方位的技术支持，帮助医院在最短时间内控制安全事件对系统造成的影响，确定安全事件的故障源及问题的原因，并提供解决方案。提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助医院快速止损，最大化降低安全事件带来的影响。

应急响应服务包括远程应急响应服务和现场应急响应服务，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：在我院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：我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）安全通告：将最新最严重的网络安全问题以最快的速度通报给我院，并且给出相应的解决办法。

在接到医院的安全事件紧急救援服务请求后，须有相应安全工程师立即响应，对安全事件进行排查，对应急响应事件须2小时内达到医院现场处置。每逢各大节假日和重大安全保障活动期间提供安全工程师驻场服务。

**产生文档：**安全事件响应服务报告

**服务频率：**按需/年

## 3.5安全设备日志分析

从安全设备各节点获得日志文件，通过人工加工具的分析方法，形成日志分析报告。该报告与定期评估结果、定期策略分析结果进行综合分析，找到当前的系统及网络设备中存在的问题和隐患，并给客户提供专业的增强建议。

1）日志收集 需定期统一收集各个安全设备的日志和报表进行存档以便分析。

2）分析日志 根据医院设备的具体情况，分析关键服务器、安全设备等设备的日志, 采取审计分析方法对日志信息进行综合分析,找到当前的系统及网络设备中存在的隐患和被攻击痕迹。

3）生成报告 根据以上评估，生成具体的日志分析报告，结合医院网络构成及业务流程等，为医院出具专业报告，并针对报告中的各项问题，提供修补建议，使发现的问题能尽可能早的得到解决，避免引起更大范围的影响和损失。

**产生文档：**日志分析报告

**服务频率：** 1次/年

## 3.6 等保咨询服务

信息安全等级保护是国家信息安全保障的基本制度、基本策略、基本方针。开展信息安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障，是信息安全保障工作中国家意志的体现。

在本项目服务期内，协助医院收集测评所需资料，配合整改必要的配置策略，提供专业的整改建议，帮助医院顺利通过等保测评。

## 3.7 系统漏洞修复

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本项目服务方提供，医院无需为该工具支持额外费用。

配合医院维护人员进行系统漏洞修复工作，该工作需要评估修复带来的潜在风险和保障修复后系统正常稳定运行。

**产生文档：**脆弱性评估报告

**服务频率：**按需/年

## 3.8 安全设备配置适应性调整

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；必须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. 业务主机、终端设备等系统的配置变更，包括基本安全配置检测和优化、系统安全检测和增强、系统升级和补丁安装。
7. 在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。

**产生文档：**安全设备配置变更实施记录

**服务频率：**按需/年

## 3.9 制度完善服务

遵从等级保护2.0、ISO27000的合规要求及网信、卫生健康局等监管单位相关要求，完善缺失制度，并协助完成政策变动所需的管理制度的梳理及补充工作；协助医院完善整体的网络安全管理制度体系。

**产生文档：**新增管理制度

**服务频率：**按需/年

## 3.10 网络安全规划建议

根据维护期间发现的安全隐患与运维工作成果，为医院提供全院网络安全建设规划与安全整改建议。

**产生文档：**网络安全规划方案

**服务频率：**1次/年

## 3.11 安全培训

从目前信息安全案件的分析来看，人员的安全观念，系统管理员的实际安全知识直接影响到整个系统安全状况。而一个安全的网络系统的保护不仅和系统管理员的系统安全知识有关，而且和领导的决策、工作环境中每个员工的安全操作等都有关系。因此，安全服务提供商需提供高质量的安全培训服务。

编写安全培训计划并经过医院方批准后实施。

编写培训教材并提交医院方审核。

组织安排相关资源进行培训的开展，包括培训讲师、培训场地等。

**产生文档：**培训记录、培训内容的文档、PPT 等产出物

**服务频率：**2次/年

**四、 项目服务要求**

1. **项目服务期限**

项目服务期限为一年。

1. **服务人员要求**

▲1）服务方应为本项目在惠亚医院成立服务小组,派驻本项目的实施技术人员和项目经理固定，如有变更，用户同意确认，服务方应组建不少3人的项目实施技术服务团队：其中1人为项目经理，1人现场驻点运维，1人二线支持。

▲2）项目经理要求：具有至少五年类似的安全服务工作经验并担当服务经理，具有有效的中国网络安全审查技术与认证中心颁发的CISAW证书和具有项目管理协会颁发的PMP证书。

▲3）需常备1名驻场安全运维管理工程师和1名机动安全专家协助医院安全运维，对安全设备策略配置变更，以及设备性能调试、故障的处理，以便于在紧急情况或工作量较大时，可随时抽调熟悉相关环境的工程师进行补充。技术人员具有有效的中国网络安全审查技术与认证中心颁发的CISAW证书、具有有效的中国信息安全测评中心颁发的CISP(注册信息安全人员证书)等相关技术资格证书。

▲4）服务方须具备具有中国信息安全测评中心颁发的信息安全服务资质认证（风险评估服务）二级及以上证书。

▲5）服务方具有中国网络安全审查技术与认证中心颁发的风险评估服务资质二级及以上证书。

▲6）服务方具有中国网络安全审查技术与认证中心颁发的信息安全应急处理服务二级及以上证书。

▲7）服务方具有中国网络安全审查技术与认证中心颁发的信息系统安全运维服务二级以上证书。

8）服务方具有ISO27001:2013（信息安全管理体系认证）。

9）服务方须具有获得ISO20000信息技术服务管理体系认证证书或以上证书。

1. **实施要求**

（1）编写项目总体安全服务方案，对各项工作的内容、方法、时间进行描述；

（2）对在项目实施中需要协调和协助的工作，需至少提前一周书面通知相关岗位人员，以便有充分的时间安排时间和业务协调；

（3）项目实施中所有的文档：过程数据、会议纪要、过程文档、计划、方案、策略等，必须以电子、纸制同时保存；

（4）项目实施中对信息系统采用的任何技术检测（本地核查、网络扫描、安全分析、设备调研）手段和方法，必须事先提交详细的实施（检测）方案，明确检测内容、方法、使用的规则（策略）、可能引发的后果、以及后果的处理等内容，经确认通过后方可进行实施；

（5）按时完成本年度信息安全联合检查工作各阶段要求的上报材料（如，工作计划、实施方案、核查表等）并准时提交；

（6）为保证用户单位信息系统安全，签署保密协议。所有与项目的有关之文档，不得泄露与第三方。

1. **应急响应要求**

▲（1）提供7\*24小时应急响应服务，在发生网络安全事件要提供技术支持。

▲（2）在出现紧急事件时，接到报告后，以最快的速度(2小时内)派遣安全技术工程师到达现场协助处理问题，技术支持人员在解决故障时，要最大限度保护好数据，做好故障恢复的文档，力争恢复到故障点前的业务状态。

1. **行为规范要求**

（1）服务方派驻人员需要严格遵守用户单位的规章制度，严格按照用户工作作息，适时进行机动值守任务。同时应遵循医院信息中心的相关管理规定。

（2）服务方与用户单位其他各合作方在协同工作时，积极配合。所有实施方案与计划需等到医院信息主管部门书面同意，再确定实施与否。

（3）遵守保密原则。按双方保密协议执行。

1. **服务资源要求**

（1）用于信息安全服务的检测设备由服务方负责提供。因项目需求增加的人力资源与其他成本，医院不另行支付费用。

1. **项目验收要求**

完成招标文件要求的所有项目和内容，有相关输出结果，并得到院方确认。

1. **付款方式**
2. 合同签订后10个工作日内，采购人向中标人支付合同总额的50%；
3. 本年度维保服务满1年后10个工作日内，屏相应的服务验收报告经甲方签字确认后，甲方向乙方支付合同总额的50%。
4. 乙方必须向甲方出具合法有效完整的完税发票及凭证进行支付结算。

**五、遵循的政策法规及行业规范**

**（包括项目服务过程中，国家最新颁布之适用的网络安全法规与行业标准）**

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《中华人民共和国网络安全法》

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术 网络安全等级保护基本要求》（GB/T22239—2019）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息系统等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全等级保护实施指南》（GB/T 25058-2019）

《信息系统安全等级保护测评准则》（GB/T 28448-2019）

《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）

《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）

《信息安全技术 操作系统安全技术要求》（GB/T20272-2019）

《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2019）

《信息安全技术 服务器技术要求》（GB/T21028-2007）

《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）