**珠海市第五人民医院网络安全设备及安全服务租赁目标及需求**

**一、 项目背景**

信息安全等级保护制度是国家信息安全保障工作的基础，也是一项事关国家安全、社会稳定的政治任务。

目前，我院信息化应用水平较前期得到较大提升，信息化在提升医疗服务效率、保障医疗质量方面发挥着较为重要的作用。随着信息化的发展，院内服务器网络设备、电脑自助机、医护交互等智能终端设备、业务系统等数量快速增长。面对日益复杂的网络环境，医院现有安全设备已无法提供基本的安全保障，医院整体性网络信息安全规划变得十分重要和迫切。

我院现有安全设备6台，其中：1台华为防火墙，采购时间为2013年，另有绿盟防火墙、IPS入侵检测、堡垒机、日志审计、数据库审计各1台采购时间为2017年。以上设备均已过期过保。

2019年，我院通过等级保护1.0的测评，备案系统包括HIS和LIS两个主业务系统。相关的安全设备：防火墙、堡垒机、日子审计、数据库审计、入侵防御检测IPS、网页防篡改（1个网站点）。

2021年5月，我院信息系统整体更换后，尚未进行相应的等保测评定级，根据国家政策对医院信息安全的要求，我院急需对于病历、HIS、LIS、PACS等4个核心系统开展等保第3级定级工作。

为有效保障等保定级工作顺利开展，我院将根据三级等保评测标准，对医院现状进行差异分析及评估，根据差评报告，对标建设，提高系统安全防护能力，降低被攻击的风险。因此，**我院安全等保项目建设一是要满足等保第3级评测要求，二是要满足我院整体安全性目标。**

**二、建设目标**

**目标：**根据计算机等级保护2.0测评标准，对病历、HIS、LIS、PACS等核心业务系统进行三级等保改造，根据评测差异报告，对标建设，提高信息系统安全防护能力，降低系统被各种攻击的风险。

**重点实现：**

**目标一：实现核心业务系统等保第3级定级；**

**目标二：建立“**技术+管理+服务**”，完善的安全技术防护体系**

根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的有关规定要求，建立满足等级保护要求的安全技术防护体系。 通过项目建设，达到医院网络信息管理的整体性安全，包括不限于**桌面终端管理安全**、**网络终端安全、内部应用安全、互联网外部安全、信息数据等资源安全、人员操作及运维安全、自助机、大屏等接入设备安全、监控摄像安全以及弱电系统的整体性安全**；

**目标三：建立零信任安全架构，实现“攻击进不来，文件拿不走，信息看不懂，数据丢不了，行为赖不掉”**，实现业务系统供应链安全，形成较强风险应对能力的安全闭环体系；

**目标四：建立以IP 为基础的统一的一体化网络管理平台**

整合数据、语音和图像等多种端到端业务场景，支持多协议、多业务、安全策略、流量管理、服务质量管理、资源管理。优化医院整体门诊楼、急诊楼、住院楼及行政楼的网络架构，构造高可靠、高稳定的无阻塞访问网络，网络设计不仅要体现当前网络多业务服务的发展趋势，同时需要具有最灵活的适应、扩展能力。

**目标五：**建立符合医院实际的应急响应机制，能迅速应对突发网络安全事件，建立健全信息**安全管理制度**；

根据网络安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。

**目标六：构建数据安全分类管理的安全体系。**实现数据采集、传输、存储、处理、交换、销毁全过程安全治理；

通过数据安全治理，明确内部数据资产，明确内部人员角色、工作责任和重要数据相关的业务流程，识别数据安全风险以及内部威胁，综合技术和管理、制度等，实现数据全生命周期的防护，确保数据资产能长期有序地、可持续地得到管理与保护，最终构建出高效稳定持久的**数据安全防护体系**。

**目标七：**达到国家电子病历五级规范建设要求，院内外医疗数据交互符合安全性；

**目标八：**达到互联互通成熟度标准化建设要求，信息系统数据共享符合安全性；

**目标九：**达到智慧医院管理，智慧医院服务评测要求，提高医院防护能力，以保障医疗业务的稳定正常开展。

**三、项目建设依据**

国家政策对网络信息安全的要求：

（1）2017年，《中华人民共和国网络安全法》的正式实施，标志着等级保护2.0的正式启动。网络安全法明确“国家实行网络安全等级保护制度。”（第21条）、“国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”（第31条）。

根据《网络安全法》要求医院属于关基部门，涉及人民群众重要的个人信息，必须依法保障医院网络信息安全，落实“网络安全等级保护制度”，“用户信息保护制度”，“关键信息基础设施重点保护制度”；

（2）国家电子病历评审规范建设，要求院内外医疗数据交互符合安全性要求；

（3）互联互通成熟度标准化建设，要求信息系统数据共享符合安全性；

（4）智慧医院管理，智慧医院服务评测要求，医院必须提高自身的防护能力，以保障医疗业务的正常开展。

（5）2022年，国家卫生健康委关于印发《三级医院评审标准（2022年版）》及其实施细则的通知，国卫医政发〔2022〕31号规定了重要业务系统必须达到等保三级标准才满足三级医院评审标准中对于网络安全的要求。

（6）《信息系统安全等级保护管理办法》

信息系统安全等级保护管理办法（以下简称“等级保护制度”）作为信息安全系统分级分类保护的一项国家标准，对于完善信息安全法规和标准体系，提高安全建设的整体水平，增强信息系统安全保护的整体性、针对性和时效性具有非常重要的意义。等级保护制度规定国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

**四、安全建设需求**

安全等保项目建设总体需求，一是满足等保第3级评测要求，二是满足我院整体安全性目标。

**4.1 整体性需求**

医院网络信息安全建设的设计实现，至少满足以下两点：

1. 安全设计实现具有整体安全性，科学合理，能够切实降低系统被攻击风险；
2. 后期安全管理运维工作具有便捷性，能够解决医院在安全运维管理中，人力资源的有限性和软硬件设备，资源的复杂性之间的需求矛盾。

**4.2功能性需求**

本方案将针对医院目前存在的各个风险点做相应的规划设计，以逐步建立健全我院网络安全防护体系，安全项目建设至少要达到以下的功能性要求：

1、根据等保测评差评报告，对标建设，完成病历、HIS、LIS、PACS等核心业务系统等保第3级定级。

2、**建立零信任安全架构，实现“攻击进不来，文件拿不走，信息看不懂，数据丢不了，行为赖不掉”**，实现业务系统供应链安全，形成较强风险应对能力的安全闭环体系；

3、建立符合医院实际的应急响应机制，能迅速应对突发网络安全事件，建立健全信息**安全管理制度**；根据网络安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。

4、**建立以IP 为基础的统一的一体化网络管理平台，实现终端安全管理**

目前，医院桌面终端数量增加，约850台终端设备（含自助机等终端设备），计算机，自助机、网络终端等缺乏有效的安全管理及防护设备，内外网的终端、服务器等无有效的准入机制统一管理，手动资料的完整性，连贯性不佳。一旦爆发病毒（如勒索病毒）将很快传染扩散，一旦内网某台终端被黑客控制，很容易进行内网攻击。

通过项目建设，全网终端实现统一的准入审核管理，统一分配IP，端口、服务等，根据医院管理要求，可出具网络资源相应报表记录，并有效记录终端，接入层，汇聚层，核心设备，服务器等重要配置信息变化，以及操作人员日志等，留痕，重要操作有记录，主动报警；

实现桌面终端管理安全、网络终端安全、内部应用安全、互联网外部安全、信息数据等资源安全、人员操作及运维安全、自助机、大屏等接入设备安全、监控摄像安全以及弱电系统的统一安全管理安全；

设计实现应整合数据、语音和图像等多种端到端业务场景，支持多协议、多业务、安全策略、流量管理、服务质量管理、资源管理。优化医院整体门诊楼、急诊楼、住院楼及行政楼的网络架构，构造高可靠、高稳定的无阻塞访问网络，网络设计不仅要体现当前网络多业务服务的发展趋势，同时需要具有最灵活的适应、扩展能力。

**5、实现内外网隔离**

通过边界隔离能力来实现内外网络进行安全数据通信，在保障用户信息系统安全性的同时，最大限度保证医院应用的方便性。

在内网和外网核心交换机之间，通过软硬件等策略，实现内外网的安全隔离，实现对网络层/OS层已知和未知攻击的全面防护能力，保护可信网络免遭黑客攻击。

6、**实现外部攻击主动防御**

有效防护外部网络攻击，对网络入侵行为的实现智能监控和防护，并及时给予主动提醒和警报，如手机短信，微信等消息提示；通过边界防护能力来实现网络攻击的识别与阻断，确保医院内部网络具备网络攻击防护能力。

对网站入侵行为的监控和防护问题，通过网站安全监控服务实现对安全监测、安全防护能力，打造可靠、安全、高效的在线服务网站，提升网站公信力。

7、**实现内部应用及终端主动防护和检测功能**

实现院内所有终端的安全防护和检测，包括网络终端、桌面终端、自助设备、大屏、监控设备等；

通过终端安全与管理能力来实现终端设备的安全管理能力，业务终端提供体系化安全防护能力，持续开展基于数字化指标的安全运营。

8、**实现网络流量监控和审计**

严格控制互联网进出口数据，实现医疗数据的安全管理，确保医疗数据不泄露，不被非法篡改，以“最小网络运行”；

9、**实现有效的数据恢复能力和备份机制，能够快速恢复重要数据，保证数据安全性**

安全防护需要跟数据保护紧密相结合，有完整的防护体系还需要有完整的备份机制来支撑，守护医院数据安全最后一道防线。

通过数据备份实现重要数据的备份，保证在发生勒索病毒加密、数据丢失、数据库误操作等数据损毁情况下，能够快速恢复重要数据，保证数据安全性。

应根据三级等保要求，建立相应的数据备份机制，对系统普通数据、核心数据、关键核心数据等分类管理，并提供院内异地数据备份功能。

10、**实现全网设备的可视化管理**

实现信息网、监控网、门禁网等医院存在的网络设备的统一规划与管理，实现可视化网络管理，能实时监控并查看全院网络现状，在网络出现回路，断网，停机，报警，拥塞等情况时，可给予及时的提醒和界面指示，并配置相应资产情况，以及权限管理；

11、**规范使用人员上网行为，实现上网行为的审计、检测及预警**

通过上网行为管控能力来实现对终端用户的互联网访问行为监控和阻断。

12、**实现对院内网络环境的态势感知能力，以及对攻击进行关联分析和溯源，保留非法侵入日志，异常操作等痕迹；**

通过态势感知能力来实现外部攻击威胁的监测、预警及处置，使安全防护和管理工作规范化流程化进行，最终通过大屏展示将网络安全态势呈现给医院。

在本院中心机房部署一套态势感知平台，并在本地重要网络节点部署潜伏威胁探针，以合规性安全要求为支撑，面向等级保护、安全管理制度和安全应急体系等建设任务，聚焦网络安全能力提升，整合组织人员、协同机制、管理制度、事件处置流程、工作流程、安全服务等方面，向组织提供统一安全能力、安全运营管理效率及安全运维效果的提升，在态势感知平台的统筹下实现联合同步防御，打通威胁感知、运维保障、监测预警、应急响应等各环节，实现各安全组件共享威胁情报和知识库，协同执行防御任务，大幅度提升整体网络协同防御能力。

态势感知平台聚焦在打造四维安全闭环能力特点的安全运营中心，即安全监测与感知、深度分析与展示、智能决策与评估、协同响应与处置的安全运营中心，辅助院内信息科发现问题、分析问题、评估问题、处理问题。

13、**实现全院供应链安全**

实现软件供应链安全，在设计实现中各项安全能力所包含的设备、工具、软件等辅助手段，均使用国产化产品，并保证产品在投入使用前经过严格的安全测试，投入使用时不存在安全漏洞，不会造成新的网络安全风险点。

14、**实现全网的安全运营管理**

通过安全运营服务，依托现有的安全设备和本方案包含的安全能力，开展各项网络安全防护工作，全面保障医院网络环境的安全。

实现第三方运维管理、账户权限、密码管理、介质管理、恶意代码防范管理、数据备份管理等日常安全运维和管理。实现资产台账信息，增加服务器、终端、网络和安全设备等信息等多种安全管理要求。

实现对科室人员防火墙、防病毒、防攻击、安全运维等网络安全专业技能培训，提高网络安全、终端安全使用相关的知识与技能。

1. 实现关键设备冗余、链路/网络冗余和重要业务模块冗余

关键设备冗余，包括支持单板热拔插、冗余控制模块、冗余电源。冗余网络设计，包括双机热备，链路冗余、链路聚合。为医院网络提供多种冗余技术，以及高效、负载均衡的备份机制。

**16、实现网络安全域划分**

根据医院实际网络情况和安全需要，结合分等级保护的思想，将医院整体网络分为内网与外网，内网划分为数据中心区域、安全运维区域、容灾区域、内网核心交换区域、内网终端业务区域；外网划分为互联网出口区域、DMZ区域、外网终端业务区域、外联区域。

并根据不同区域的安全性要求给出具体的设计方案及图示说明。

（**互联网出口域：**需在互联网出口边界进行隔离和访问控制，保护内部网络，从2-7层对攻击进行防护，实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击，利用网络防病毒，主动扫描web和电子邮件流量、阻止恶意软件到达并感染网络上主机等防护功能；需对互联网出口流量进行识别并对流量进行管控，提高带宽利用率的同时保障用户上网体验，并按相关法律法规进行上网行为审计。

**外联区域：**与对端政务网/内网安全平台数据对接，需识别内网之间流量中的威胁，实现对流量中入侵行为的检测与阻断。

**内外网终端业务域：**安全域内的终端上需具备防恶意代码的能力；需满足健康一体机、移动家庭医生签约等移动办公需求，实现安全可靠的网络接入。

**DMZ区域：**该安全域内主要承载对外提供服务的服务器等，包括门户网站前端服务器、预约挂号系统等，外网接入用户需满足身份验证、数据加密传输的要求。需在DMZ区域边界设置访问控制策略，并具备应用层攻击检测与防护能力。

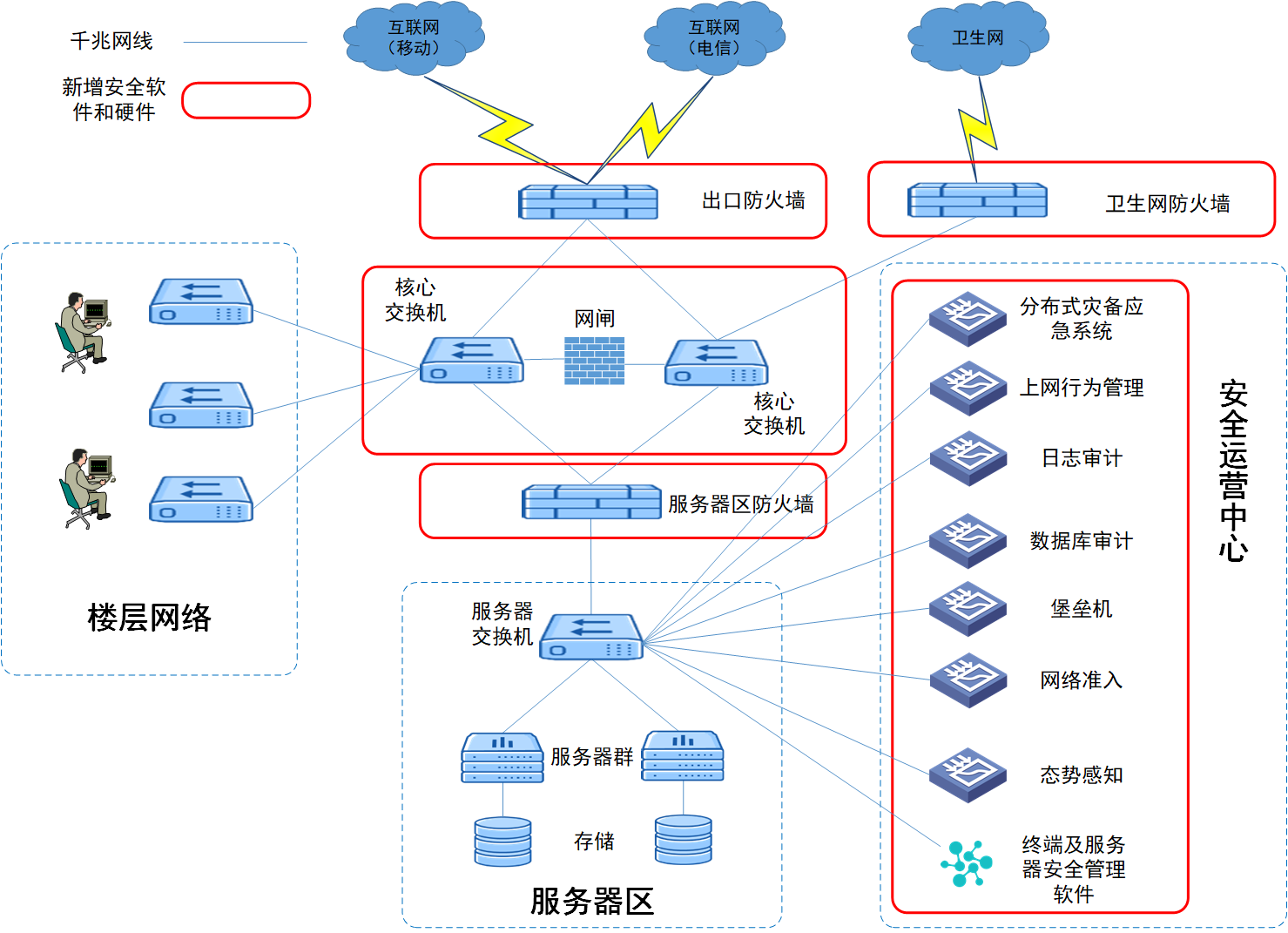
**数据中心区域：**该安全域主要承载内网核心业务信息系统，需对这些业务信息系统提供2-7层安全威胁识别及阻断攻击行为的能力，如网页防篡改、SQL注入、XSS（跨站脚本攻击）、CSRF（跨站请求伪造攻击）、cookie篡改等。

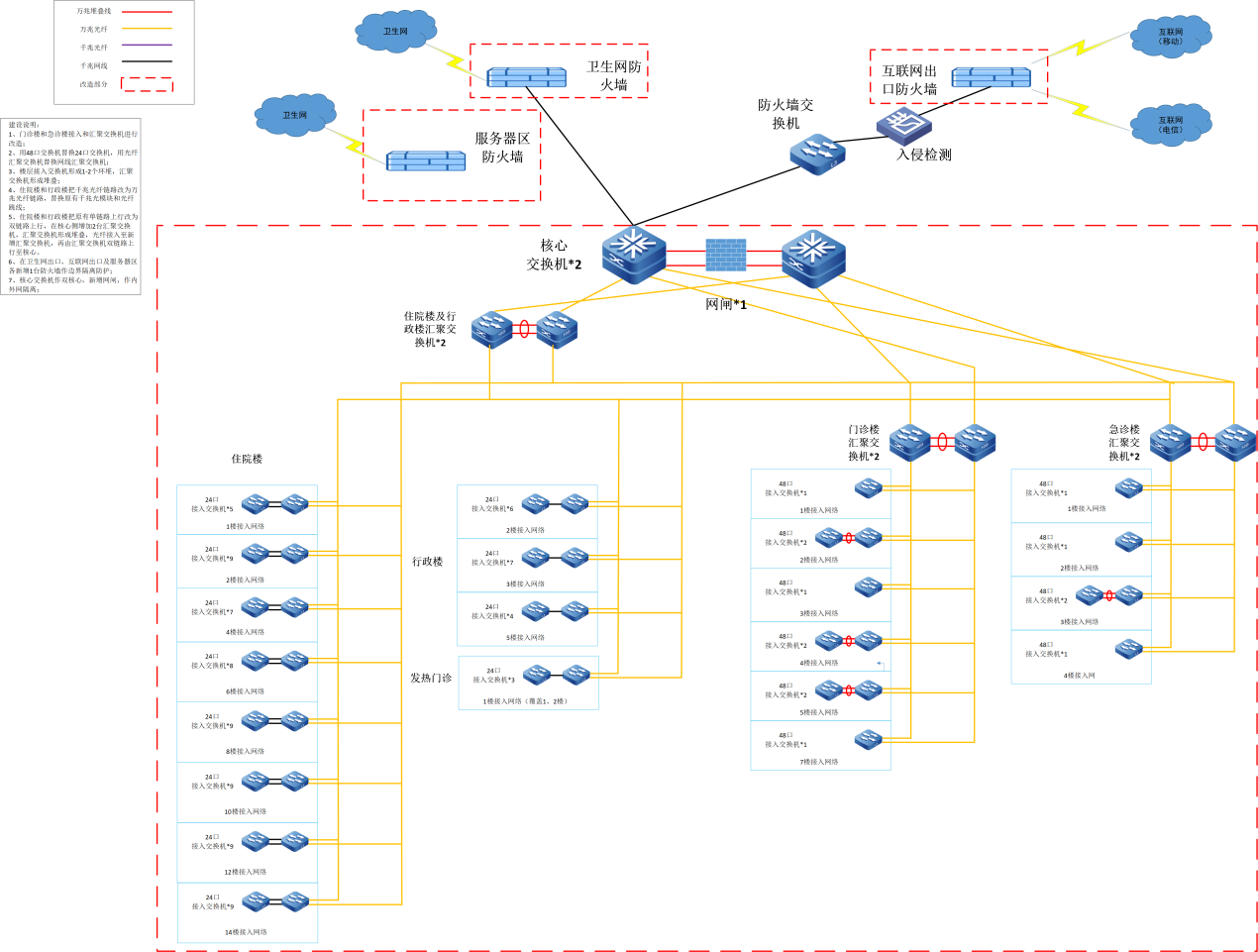
**安全运维区域：**统一部署日志审计系统，堡垒主机，漏洞扫描系统，终端准入系统、数据备份等安全防护措施。同时部署态势感知，通过大数据分析，发现未知威胁及可视化展示。）

17、**满足电子病历五级评审中，对于安全建设的要求。**

18、**满足互联互通四级甲等评测中，对于安全建设的要求。**

**五、网路拓扑图（初步计划，可根据医院实际网络架构调整）**





**六、内容及技术要求**

**1.专业基础设施服务**

基础设施服务，安全设施租赁服务包含（但不限于）：外网出口防火墙2台，内网防火墙1台，内网数据中心WAF 2台，外网上网行为管理2台，内网上网行为管理1台，零信任安全访问系统1台，数据库审计1台，日志审计1台，堡垒机1台，网闸2台，物联网与网络安全监测响应平台1台，流量采集探针1台，终端安全管理平台1套，备份一体机1台，网络管理平台1套。主要网络及安全设备日志保存六个月以上，项目涉及租用的设备及平台符合信创要求，并提供相关证明材料或者承诺。

安全设施租赁要求满足：

（1）服务期内各规则库升级许可服务，租赁设备的软硬件及功能模块规则库更新在合同履行期限内均在质保期内；

（2）各设备原厂商提供相应的技术咨询及指导服务，对设备的常规使用进行培训；

（3）工作日设备每日巡检服务；

（4)提供故障维修服务，出现故障安排服务人员上门更换硬件或配件，确保设备正常运行，备机备件实时更换服务；

(5)7\*24应急响应服务，设备故障响应时间≤30分钟。

（6）主要网络及安全设备日志保存六个月以上。

（7）硬件需与医院内部的系统相适配，如与现有系统不适配则需无条件更换至适配为止。

（8）满足采购人3年业务所需。

专业基础设施服务主要基础设施（包含但不限于）租用如下：

设备租用清单

| **序号** | **名称及类别** | **设备配置要求** |
| --- | --- | --- |
| 1 | 外网出口防火墙（编号1-2）租赁服务 | 2台。双电源，网络层吞吐量≥20G，应用层吞吐量≥9G，防病毒吞吐量≥1.5G，IPS吞吐量≥1.3G，并发连接数≥200万，HTTP新建连接数≥9万。功能模块：系统管理、身份认证、攻击防护、高可用、病毒防护、IPS。 |
| 2 | 内网防火墙（编号3）租赁服务 | 1台。双电源，网络层吞吐量≥10G，应用层吞吐量≥5G，防病毒吞吐量≥1G，IPS吞吐量≥800，并发连接数≥200万，HTTP新建连接数≥6万。功能模块：系统管理、身份认证、攻击防护、高可用、病毒防护、IPS。 |
| 3 | 内网数据中心WAF（编号4-5）租赁服务 | 2台。双电源，网络层吞吐量≥35G，HTTP应用层吞吐量≥20G，HTTP新建连接数≥18万，HTTP并发连接数≥410万，SFP+。功能模块：系统管理、身份认证、攻击防 护、高可用、病毒防护、IPS。 |
| 4 | 外网上网行为管理（编号6-7）租赁服务 | 2台。双电源。网络层吞吐量≥10Gb，应用层吞吐量≥1.5Gb，带宽性能≥1Gb，每秒新建连接数≥14000，最大并发连接数≥600000。 |
| 5 | 内网上网行为管理（编号8）租赁服务 | 1台。双电源，网络层吞吐量≥3.6Gb，应用层吞吐量≥450Mb，带宽性能≥300Mb，每秒新建连接数≥4000，最大并发连接数≥150000。 |
| 6 | 零信任安全访问系统（编号9）租赁服务 | 1套。替换符合国产化要求硬件平台。提供安全运营平台软件基础功能（含态势感知、工单系统、运营监管等），包含日志采集、报表、资产管理、威胁告警管理、风险评估、脆弱性管理、威胁预警、工单、调查分析-基础、调查分析-攻击链分析、搜索、态势首页、外部威胁态势感知、安全运营态势感知、资产风险态势感知、全网漏洞态势、知识库、系统管理功能。默认提供3台服务器集群节点安装授权。 |
| 7 | 数据库审计（编号10）租赁服务 | 1台，替换符合国产化要求硬件平台。  最大硬件吞吐量≥2Gbps，最大纯数据库流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥30000条SQL/s，日志检索性能≥500000条/秒。内存≥8G，硬盘容量≥2T，电源：冗余电源。 |
| 8 | 日志审计（编号11）租赁服务 | 1台，主机审计许可证书数量≥200，最大可扩展审计主机许可数≥450，可用存储量≥4TB，平均每秒处理日志数（eps）最大性能≥3500。规格：2U，内存≥32G。 |
| 9 | 堡垒机（编号12）租赁服务 | 1台，运维授权数≥200，最大可扩展资产数≥1000，图形运维最大并发数≥200，字符运维最大并发数≥350，硬盘容量≥2T 。 |
| 10 | 网闸（编号13-14）租赁服务 | 2台，吞吐量≥1Gbps，并发连接数≥10W，2U设备，冗余电源。支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。 |
| 11 | 物联网与网络安全监测响应平台（编号15）租赁服务 | 1台，存储容量≥14.4T，内存≥96GB，数据盘≥4\*4TB，电源：冗余电源。 |
| 12 | 流量采集探针（编号16-17）租赁服务 | 2台，网络层吞吐量≥1.5Gbps，应用层吞吐量≥500Mbps。硬盘容量≥256GB SSD。 |
| 13 | 终端安全管理平台（编号18）租赁服务 | 1套，授权：PC授权1300个，服务器版授权200个，使用统一的控制平台管理。 |
| 14 | 备份一体机（编号19）租赁服务 | 1台，硬件参数：2U机架式备份软件专用存储服务器，12个3.5英寸盘位； 2）CPU≥2颗Intel 4310 CPU（主频 2.1GHz，单颗 CPU 12 核）； 3）内存≥ 64GB高速缓存；4）系统盘≥ 2块960G SSD；5）数据盘≥100T可用存储空间；6）网络≥板载标配4个千兆网络端口和2个万兆光口（含光模块）；7）可支持不少于5个PCI扩展（包括8GB 16GB FC HBA卡，1GE或10GE网络接口卡）；8）双冗余电源。  授权配置参数：1）配置≥100T定时容量授权许可；2）配置不限备份客户端数量的永久增量备份代理授权许可；3）配置不限容量重复数据删除代理授权许可；4）配置CDP 持续数据保护场地授权代理许可；5）配置不限文件数量备份恢复功能；6）配置不限操作系统数量备份恢复功能。 |
| 15 | 网络管理平台（编号20）租赁服务 | 1套，授权：包含≥100节点授权 |

**2.网络安全运营服务**

网络安全运营服务，包含安全咨询服务、安全评估服务、安全加固、应急响应服务、安全应急演练服务、渗透测试服务、医院官网、APP/小程序深度评估服务、安全培训服务、安全现场服务、应急护网服务、关基设施安全检测和风险评估服务。具体如表格所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **服务内容** | **服务要求** |
| 1 | 安全咨询服务 | （1）以现场服务的方式，进行安全咨询规划，主要内容为安全管理体系规划、安全技术体系规划、安全运维体系规划，达到了深刻认识安全体系建设，顺利通过等级保护2.0中安全管理要求。 | （1）顺利通过等级保护测评  （2）明确关键信息基础设施安全建设需求  （3）完善安全管理体系建设 |
| （2）基于《关键信息基础设施安全保护条例》，协助完成医院关键信息基础设施保护方案，每年对关键信息基础设施系统进行风险评估并出具报告。 |
| （3）以《网络安全法》《网络安全等级保护基本要求》为依据，结合医院有关要求，对关键信息基础设施、信息安全、信息化建设等情况进行调研分析，协助完善医院网络安全及关键信息基础设施相关制度；协助梳理医院资产情况和存在问题，输出相关的资产台账。 |
| （4）安全运维体系规划服务，从风险评估、安全审计、日常维护、信息资产、口令、电子文档、系统应急等方面对运维过程中的重要管理问题进行安全管理建设，进行全方位的、系统的运维保障管理和技术体系的应用。 |
| 2 | 安全评估服务 | （1）协助医院每月完成本地和云上信息系统的安全漏洞扫描工作，通过专业软件和人工分析梳理每个系统系统存在安全漏洞，并出具相关网络安全漏洞扫描报告。 | 每月输出漏洞评估报告、针对高频类型漏洞进行专项人工复测，使安全风险降到最低 |
| （2）按要求根据省委网信办、省公安厅、政务数局等国家或广东省网络安全部门通报存在漏洞的系统进行安全漏洞风险复查，并对这些漏洞进行分析研判，确认其对医院造成的风险，并提出优化方案和指引。 |
| （3）采用最佳配置核查实践对操作系统、数据库、中间件、网络设备、网络安全设备、网络边界进行配置核查。 |
| （4）专业安全顾问进行访谈、网络安全现状评估等 |
| 3 | 安全加固服务 | 按评估结果对相关网络资产设备及系统通过升级、打补丁、修改配置等整改的技术支持。 | 对重要资产设备进行加固，每季度，共4次/年 |
| 4 | 应急响应服务 | （1）重大会议和节假日期间，组织技术人员协助医院做好值班工作，保障重要时期的业务系统和网络的安全稳定，并根据需要完善相关的保障方案。 | 能够快速定位安全风险，在准确判断安全事件原因的基础上；提出基于安全事件整体安全解决方案；排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置，达到了针对客户业务系统能够快速定位重要业务系统，并进行溯源反制的能力 |
| （2）协助医院及时处置日常网络安全问题，在指定时间内（30分钟内响应，1小时到达现场，4小时内排除故障）响应和处理完成应急事件，包括故障查因、事件跟踪、系统恢复，使网络和信息系统在最短时间内恢复正常运作，根据出现的事件，输出相关排查报告。 |
| **5** | 应急攻防演练服务 | 为医院系统开展网络应急攻防演练服务。 | 通过演练能够发现医院系统网络安全存在的薄弱环节（具体演练时间以采购人发出通知为准） |
| 6 | 渗透测试服务 | 以模拟黑客方式对互联网应用系统进行渗透测试，找出安全风险，通过渗透测试发现系统不同程度的漏洞并做到了及时修补。每年对医院系统进行渗透与攻击性监测，并出具相关报告。 | 每年对医院至少4个系统进行渗透与攻击性监测 |
| 7 | 医院官网、APP/小程序深度评估服务 | 主要内容为医院官网、APP、粤政易及微信等平台上的小程序按常见的漏洞类型进行测试，达到了找出不合规API调用、漏洞类型等并修复，降低针对移动端网络安全风险。 | 找出SQL注入漏洞类型、跨站脚本漏洞类型、弱口令漏洞类型 |
| 8 | 安全培训服务 | 开展线下网络安全培训两天，人数不低于600人，培训内容包括但不限于网络安全、软件正版化、关键信息基础设施等内容。 | 提高医院工作人员网络安全意识，全面提升相关单位网络和信息系统的安全管理水平 |
| 9 | 安全现场服务 | 现场服务是日常由不少于1名专业安全人员在医院办公场所，提供广东省水利厅安全相关安全业务的运维工作，定期对系统进行安全巡检，发现系统存在的风险，提供及时的安全风险处置。现场人员需具备信息安全相关资质证书，从事信息安全相关工作3年以上工作经验。 | 协助加强网络安全日常监测 |
| 10 | 应急护网服务 | 协助医院完成国家、省、市网络安全管理部门组织的网络安全攻防演练防守工作，加派人员和设备强化医院网络安全开展应急护网演练防守和值守等相关工作，并按照演练相关要求，输出防守报告、溯源报告等材料。 | 协助做好网络安全部门组织的演练活动期间的网络安全防守工作 |
| 11 | 互联网系统云监测服务 | 协助医院完成面向政务云、互联网等重要业务系统安全监管，需要互联网系统云监测服务平台服务对业务系统进行7\*24小时的安全监测，主要方式为通过互联网系统云监测服务平台，将原有的小时级安全响应转换为分钟级响应。 | 做好政务云、互联网等重要业务系统云监测 |
| 12 | 互联网系统云防护服务 | 协助医院完成政务云、互联网等重要业务系统的安全防护，需要互联网系统云防护服务对业务进行7\*24小时的安全防护，主要内容为通过互联网系统云防护服务平台针对漏洞、暗链、黑页、钓鱼、篡改的安全防护，以及未知攻击等安全攻击防护。 | 做好政务云、互联网等重要业务系统云防护 |
| 13 | 关基设施安全检测和风险评估服务 | 按照关键信息基础设施保护条例编写工作方案，协助医院完成关键信息基础设施防护，按照要求需要每年开展安全检测和风险评估服务。协助医院编制关基系统网络安全事件应急预案。 | 协助医院完成关键信息基础设施等重要系统的防护 |