# 信息系统等级保护测评项目用户需求书

# 项目概况

根据《网络安全法》和《中华人民共和国计算机信息系统安全等级保护条例》等法律法规要求，医院的核心信息系统为关键信息基础设施，网络安全等级保护等级不低于三级的信息系统，需要每年进行等保测评，从物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度等各方面进行的安全检测评估。现对我院8个三级等保信息系统进行年度测评。

# 测评系统服务清单

|  |  |  |
| --- | --- | --- |
| **系统名称** | **证书编号** | **备案等级** |
| 电子病历信息平台 | 44001845195-00004 | 三级 |
| PACS系统 | 44001845195-00005 | 三级 |
| LIS系统 | 44001845195-00006 | 三级 |
| HIS系统 | 44001845195-00003 | 三级 |
| 广东省第二人民医院信息集成平台 | 44000045195-22001 | 三级 |
| 互联网医院系统 | 44000045195-21001 | 三级 |
| 广东省互联网医疗服务监管平台 | 44000045195-21002 | 三级 |
| 移动护理 | 44000045195-22002 | 三级 |
| 对以上8个信息系统进行测评：三级复测。  服务内容：  1、协助等保测评机构完成差距测评。  2、根据差距测评问题清单，需完成网络、网络安全设备、服务器、数据库以及管理制度层面差距整改，且协助应用厂家完成应用系统整改。  3、收集整改记录，提供给专业测评机构，完成等保测评验收且出具等保测评报告。  4、提交等保测评报告至广州市公安局公共信息网络安全综合管理系统，并收集等保测评报告提交回执单。 | | |

# 项目需求

## 项目范围

按照国家和行业的要求，广东省第二人民医院信息系统的安全配置是符合国家等级保护标准的要求。在本期服务中，服务商要提供本年度等保的全生命周期的服务，提供从差距测评、整改指导、等保验收、等保测评报告提交回执等所有等保阶段的服务。

完成医院以下信息系统等保2.0测评：电子病历信息平台、PACS系统、LIS系统、HIS系统、广东省第二人民医院信息集成平台、互联网医院系统、广东省互联网医疗服务监管平台、移动护理三级等保2.0测评。

* **系统描述**

**电子病历信息平台：**电子病历信息平台包含了医生工作站、护士工作站、会诊工作站、质控管理、病案管理、病历维护、病历浏览、病案借阅、科室质控等功能模块。

**PACS系统：**PACS系统为广东省第二人民医院所属各部门提供对病人的各种医学影像（包括核磁共振、CT扫描、超声波等设备产生的图像）的收集，存储、提取等能力，将医学图像以数字化的方式进行存储，当需要时，在一定的授权下能快速的调取使用，并增加了一些辅助诊断功能的影像归档及通信系统。PACS信息系统主要由影像处理、报告管理等子模块组成。

**LIS系统：**LIS信息系统能将实验仪器与计算机组成网络，使病人样品登录、实验数据存取、报告审核、打印分发，实验数据统计分析等繁杂的操作过程实现了智能化、自动化和规范化管理。有助于提高实验室的整体管理水平，减少漏洞，提高检验质量。主要的功能模块有：数据处理、数据查询、数据报表、质量控制、试剂管理、基本设置、系统管理等。

**HIS系统**：HIS系统为广东省第二人民医院所属各部门提供对病人诊疗信息和管理信息的录入、存储、处理、提取及数据交换的能力，并满足所有授权用户的功能需求的应用系统。

**广东省第二人民医院信息集成平台：**广东省第二人民医院信息集成平台通过系统的建设，能够达成更加科学、高效、安全的医院信息集成模式，优化各个业务系统间的数据流及业务流，新的业务系统与医院现有系统集成以及老的业务系统改造的过程会更加顺畅快捷，对各个系统的供应商的依赖程度会降低。

**互联网医院系统：**互联网医院系统主要提供广东省第二人民医院健康管理平台微信公众号，“叮呗医生+”小程序等多途径免费开展医生在线问诊AI医生智能问诊、居民个人健康管理等业务，为线上患者提供全生命周期智慧医疗健康信息服务、移动支付。

**广东省互联网医疗服务监管平台**：广东省互联网医疗服务监管平台系统主要通过对互联网医院的电子病历、处方、诊疗过程视频的监管，判断医生是否符合执业规定、互联网诊疗是否在规定范围内、诊疗行为是否符合诊疗规范、药品作用是否符合规范。广东省互联网医疗服务监管平台系统部署于广东省政务云平台，所有应用均部署于政务云平台的政务外网区。

**移动护理：**移动护理系统是医院护士提供记录与管理住院患者的有效工具。护士可以在系统内管理患者的基本信息、体征信息、医嘱信息、各类文书信息等。系统保障了日常护理工作的有序进行和留痕，减少了护士的日常工作量，推进了医院无纸化的进程

## 现网的网络安全设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **现网的网络及网络安全设备清单** | | | | |
| **序号** | **设备名称** | **品牌** | **用途** | **备注** |
|
| 1 | 网络核心交换机 | 华为 | 核心数据交换 | / |
| 2 | 服务器核心交换机 | 华为 | 核心数据交换 | / |
| 3 | 数据中心防火墙 | 深信服 | WAF、IPS防护 | / |
| 4 | 外网IPS防火墙 | 深信服 | WAF、IPS防护 | / |
| 5 | 上网行为管理 | 深信服 | 上网行为审计 | / |
| 6 | 外网WIFI防火墙 | 深信服 | WAF、IPS防护 | / |
| 7 | 互联网应用隔离防火墙 | 深信服 | WAF、IPS防护 | / |
| 8 | 终端杀毒软件 | 卡巴斯基 | 病毒查杀防护 | / |
| 9 | 日志审计 | 网安可信 | 日志审计 | / |
| 10 | 态势感知平台 | 深信服 | 日志分析平台 | / |
| 11 | 态势感知探针 | 深信服 | 流量收集风险感知 | / |
| 12 | WIFI上网认证 | 任子行 | WiFi互联网行为审计 | / |
| 13 | 互联网应用出口火墙 | 深信服 | WAF、IPS防护 | / |
| 14 | 入网规范管理系统 | 盈高 | 访问控制 | / |
| 15 | 堡垒机 | 齐治 | 安全运维 | / |
| 16 | 数据库审计 | 安恒 | 安全审计 | / |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评信息系统服务器设备数量** | | | |
| **序号** | **系统名称** | **服务器数量** | **备注** |
| 1 | 电子病历信息平台 | 4台 | / |
| 2 | PACS系统 | 6台 | / |
| 3 | LIS系统 | 2台 | / |
| 4 | HIS系统 | 4台 | / |
| 5 | 广东省第二人民医院信息集成平台 | 4台 | / |
| 6 | 互联网医院系统 | 5台 | / |
| 7 | 广东省互联网医疗服务监管平台 | 5台 | / |
| 8 | 移动护理 | 5台 | / |

## 服务要求

本项目需要按照等保2.0的流程要求，结合当前、信息系统安全建设的实际情况进行总体设计，并把整个项目分成以下4个阶段，总项目实施周期为3个月。

**项目阶段表**

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **实施内容** | **产出物** | **完成周期** |
| 等保差距测评 | 现场评测阶段通过与评测委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料 | 《系统差距测评报告》 | 20天 |
| 建设整改 | 参照《系统差距测评报告》服务方需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，且协助应用厂家完成应用系统整改 | 整改记录 | 1个月 |
| 等保验收 | 渗透测试复测，测评机构应对现场测评获得的测评结果进行汇总分析，形成等级测评结论 | 系统验收测评报告 | 1个月 |
| 项目完成 | 将系统验收测评报告提交至“广州市公安局公共信息网络安全综合管理系统” | 签收回执 | 10天 |

### （1）▲服务要求

1. 本项目包含等保测评和等保整改的费用。
2. 服务方需配合测评机构完成8套系统差距测评，督促测评机构出具《系统差距测评报告》。
3. 服务方需根据《系统差距测评报告》，需完成网络、网络安全设备、服务器、数据库以及管理制度层面差距整改。
4. 配合需求方完成应用系统层面差距清单的整改，督促测评机构出具《系统验收测评报告》。
5. 最终获取“广州市公安局公共信息网络安全综合管理系统”提供的等保测评报告签收回执。

### （2）建设整改

按照《信息系统信息安全等级保护定级指南》、《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019的要求，依据信息系统的安全保护等级，通过人员访谈、文档审查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心及备份与恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面，判断网站现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。对信息系统进行整体、全面、公正的评估，对不符合项进行风险分析，组织专家团队从以下几方面进行综合评估，从而输出《差距测评问题清单》：

1. 基础物理设施安全：保障网络周边环境和物理特性引起的网络设备和线路的持续使用。
2. 网络连接安全：保障网络传输中的安全，尤其保障网络边界和外部接入中的安全。
3. 计算环境的安全：保障操作系统、数据库、服务器、用户终端及相关商用产品的安全。
4. 应用系统安全：保障应用程序层对网络信息的保密性、完整性和信源的真实的保护和鉴别，防止和抵御各种安全威胁和攻击手段，在一定程度上弥补和完善现有操作系统和网络信息系统的安全风险。
5. 保障数据安全及备份恢复：保障数据完整性、数据保密性、备份和恢复等。
6. 安全管理体系保障：根据国家有关信息安全等级保护方面的标准和规范要求，建立一套切实可行的安全管理体系，加强安全管理机制。

指导需求方安全管理员以及开发人员按照《差距测评问题清单》进行相关系统的整改。并在整改完成后，根据《差距测评问题清单》进行验收，以保证整改措施的最终落地，获得评测机构出具《系统验收测评报告》。

### （3）项目完成

完成验收测评工作，达到国家规定的信息安全要求后，向公安部门提交《系统验收测评报告》，并拿到“广州市公安局公共信息网络安全综合管理系统”出具的等保测评报告签收回执。