# 用户需求书

## 整体要求

1.本用户需求书中标注“★”条款的，投标人必须作出响应，如作负偏离响应或不作响应的，视为无效投标处理；凡加“▲”的地方均被视为重要的技术指标要求或性能要求，如要求提供证明文件的，需提供相关证明文件，投标人要特别加以注意。

## 项目概况

### 建设背景

随着信息技术的迅猛发展，网络安全威胁变得日益严峻，各类信息系统已然成为国家安全、社会稳定以及经济发展的关键基础设施。为确保信息系统安全可控，根据国家相关法律法规和标准要求，尤其是《中华人民共和国网络安全法》《信息安全等级保护基本要求》等，本项目计划对江门市第二人民医院的信息系统进行等级保护测评（以下简称“等保测评”）。在此基础上，本项目将协助医院完成等保整改加固工作，以提升系统安全防护能力。

## 项目采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **项目内容** | **数量** | **单位** | **备注** |
| 1 | **等保测评及安全加固服务** | 互联网医院系统网络安全等保等级三级系统，一年共测评一次，包括安全加固服务。 | 1 | 项 |  |
| 2 | **安全服务** | 通过安全服务工具+人工的方式提供以下安全服务：1.资产梳理服务（包括（1）互联网资产梳理：互联网暴露面扫描、互联网域名梳理、网站可访问情况梳理、建立互利网暴露资产信息列表；（2）内部重要资产梳理：内部网络资产信息收集和整理，建立内部重要资产列表，资产画像（基于流量采集）；（3）新增资产监测：对互联网与内网的新增资产进行监测和报警。）2.漏洞扫描服务（通过安全服务工具以远程和本地扫描的方式定期对设备和系统进行漏洞扫描，对漏洞扫描结果进行验证，提供漏洞分析报告，漏洞修复建议和风险应对建议，有效地降低安全风险。）3.安全基线检查服务（采用最佳配置核查实践对操作系统、数据库、中间件等进行分析和配置核查，输出基线核查报告）4.弱口令扫描服务（对医院内部安全设备、网络设备、服务器以及终端进行弱口令扫描，提前发现系统可能存在的各类安全风险。）5.安全合规监测服务（对医院安全合规符合情况进行预评估，量化等保测评、数据安全、个人信息保护、国密合规、三甲评审、互联网诊疗、互联互通评级、智慧医院评级、电子病历评级安全部分分数，同时输出合规差距清单）服务频率：按需/年 | 1 | 项 |  |

### 服务内容要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **工作内容** | **输出内容** | **说明** |
| 安全评估阶段 |
| 1.1 | 网络安全技术安全评估 | 安全测评通用要求，安全物理环境、安全通信网络、安全区域边界、安全计算环境加相关扩展要求（如有）等进行评估分析，记录相关的评估结果。 | 现场访谈、检查、测试记录表、关键截图 | 机房现场评估（物理、主机、网络、数据），应用与数据库评估，安排相关人员配合。 |
| 1.2 | 信息系统管理安全评估 | 安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理加相关扩展要求等进行评估分析，记录相关的评估结果。 | 评估结果 | 1、提供相关管理制度（电子版或纸质版）；2、配合基本情况 调研。 |
| 1.3 | 评估和测评结果确定 | 对上一步骤成果进行确认，并协调下阶段工作（安全问题（整改）交流） | 评估结果 |  |
| 项目报告整理编写阶段 |
| 2.1 | 报告编制 | 编制《安全问题整改清单》 | 《安全问题整改清单》 | 系统运维人员配合。 |
| 安全整改阶段 |
| 3.1 | 安全整改 | 根据《安全问题整改清单》针对数据库及应用安全协助用户与系统开发商协调加固。 | 加固截图 |  |
| 3.2 | 安全服务 | 根据测评报告对相关系统的操作系统主机进行配置加固、主机漏洞扫描及修复。  | 现场访谈、检查、现场加固实施 | 相关人员配合 |
| 第二次测评阶段 |
| 4.1 | 测评实施阶段 | 针对下面相关层面开展测评：安全测评通用要求，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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理加扩展要求等. | 现场访谈、检查、测试记录表、关键截图，填写现场测评实施记录 | 1、机房现场测评（物理、主机、网络、数据），相关人员配合2、应用管理员配合操作（应用、数据），相关人员配合 |
| 4.2 | 测评报告编制阶段 | 编制《\*\*\*\*系统安全等级测评报告》，确定测评结果 | 《\*\*\*\*系统安全等级测评报告》 | 保持信息畅通，确保测评记录的真实性 |
| 4.3 | 等级保护测评报告-专家内审 | 对相关系统安全等级保护测评报告整体测评进行专家内审，审查完毕后定稿打印封装盖章 | 《\*\*\*\*系统安全等级保护测评报告》 | 保持沟通，配合相关文档盖章流程 |

**差距测评**

差距测评包括两个方面的内容：一是安全控制测评，主要测评网络安全等级保护要求的基本安全控制在系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

**验收测评**

供应商按照等保2.0的相关要求出具测评报告，协助江门市第二人民医院进行测评报告备案工作，提交验收测评报告到当地公安等级保护部门，完成报告备案工作。

**安全服务要求**

* 网络安全扫描服务

对本次实施等级保护测评的信息系统，采用专业安全扫描工具与人工检查相结合的方式进行主机安全漏洞扫描，具体内容包括主机操作系统漏洞、网络和安全设备漏洞等内容，并输出相应的安全扫描漏洞报告（内附整改建议）。

本项服务的服务频率为完成2次网络安全扫描服务，并交付漏洞扫描报告。

本项服务的服务频率为完成1次网络安全加固服务。

* 安全制度建设服务

根据医院现有的网络安全相关管理制度及对应的执行记录，指导医院完善一套第三级网络安全等级保护所需求的管理制度。

本项服务的服务频率为开展1次管理制度修订服务，并交付管理制度汇编。

* 数据安全咨询服务

通过围绕数据安全管理制度体系、数据安全全生命周期管理能力体系、数据安全运维能力体系三个纬度出发，梳理数据使用过程之中的管理体系现状和技术防护现状，从而定向解决和处理问题。从而规划建设我院数据安全总体能力体系建设

### 测评要求

按照等保2.0的相关要求对信息系统安全等级保护状况进行测试评估，包括安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

安全通用要求规定了不管等级保护对象形态如何必须满足的要求，测评单元分为安全技术测评和安全管理测评两大类，技术要求包括：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；管理要求包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

云计算拓展要求包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理。

移动互联网拓展要求包括：安全物理环境、安全区域边界、安全计算环境、安全建设管理。

物联网安全拓展要求包括：安全物理环境、安全区域边界、安全建设管理。

工业控制系统安全拓展要求包括：安全物理环境、网络通信网络、安全区域边界、安全计算环境。

### 测评方法与工具要求

#### 测评方法

**（1）人员访谈**

与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

**（2）配置检查**

利用上机验证的方式检查主机操作系统、数据库、网络设备、安全设备、应用系统等配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。

**（3）文档审查**

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

**（4）实地查看**

通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

#### 安全服务工具要求

为保障整体安全服务成效，需配备安全服务工具提供支撑，具体包括0day应用漏洞检测工具及安全合规检测工具。其中，安全合规检测工具需在本院部署并稳定运行一年，专门服务于本院日常安全合规监测工作，以上工具应满足以下要求：

**0day应用漏洞检测工具技术要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **能力要求** |
|  | **威胁检测能力** | ▲支持http、mysql、ssh、smb、ftp、远程桌面等协议的双向分析。可在同一个规则内关联分析一个TCP会话的双向报文，当请求包含有指定攻击报文，返回包含有受影响的报文时，才发出报警。在同一条报警日志中要求同时展示双向报文**（提供功能截图证明）** |
|  | **DNS检测能力** | ▲域名解析：支持对访问的所有域名进行解析和分析（包含正常的访问记录），并记录的字段包括：会话时间、来源IP、域名IP、DNS服务器IP、DNS返回记录、查询域名、协议、长度、数据源、信息摘要等。**（提供功能截图证明）** |
|  | **风险告警能力** | ▲支持提供充足证明此次告警的信息，报警内容包含完整的双向数据包，包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容，同时针对每条单独的告警下载PCAP报文。**（提供功能截图证明）** |
|  | ▲支持以网页快照形式展示服务器返回的内容。**（提供功能截图证明）** |
|  | **告警管理与回溯分析能力** | 支持通过时间、IP、Url、Post数据包、状态码、检索关键字等内容进行回溯分析，支持在回溯分析时去除含特定关键字的相关日志记录，支持复现整个攻击事件全部HTTP报文的关联分析。**（提供功能截图证明）** |
|  | 支持通过时间、IP、关键字、get参数、目的主机、日志类型、状态码等多个关键字及正则表达式的模式进行全文检索和回溯分析。**（提供功能截图证明）** |
|  | ▲支持存储全量的Web应用交互双向数据包，包含正常交互的http日志数据包，且有单独页面展示，http日志数据包需包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容。**（提供功能截图证明）** |
|  | **漏洞检测能力** | 支持扩展漏洞检测模块，可自主扫描操作系统及网站漏洞。包括缓冲区溢出、SQL注入、跨站脚本漏洞（XSS）、信息泄漏等常见的Web应用漏洞。 |
|  | **自定义检测规则能力** | ▲可按域名主机关键字、URL关键字、文件名关键字、请求报文等关键字进行发包请求规则设置；可按源IP、目的IP、HTTP状态码、返回报文等关键字进行返回包规则设置。**（提供功能截图证明）** |

**安全合规检测工具技术要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **功能要求** |
|  | **授权许可** | 提供无授权限制的资产管理功能授权许可，资产包括主机、网站、物联网设备、端口等**（提供功能截图证明）** |
| ▲提供无授权限制的主机漏洞扫描、漏洞管理功能、WEB扫描功能、基线配置核查功能、弱口令检测功能授权许可。以上功能授权许可提供界面截图证明。**（提供功能截图证明）** |
|  | **资产发现探测** | ▲支持自动扫描IP资产信息，包括：设备名称、IP、设备类型、MAC、发现时间等资产指纹特征；支持识别资产端口/弱口令信息，端口信息包括：IP、端口、传输协议、应用协议、版本、状态；弱口令信息包括IP、端口、服务协议、用户名、密码。**（提供功能截图证明）** |
|  | 通过爬取单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址。 |
|  | **资产深度管理** | 可及时发现未存活IP、未存活端口以及访问延迟的网站，可查看未存活IP列表、未存活端口列表，可对未存活的资产进行移除操作 |
|  | 可按最近一周、最近一个月、最近一个季度可查新增的主机IP资产、网站资产，掌握资产新增趋势 |
|  | **网站风险监测** | 支持网站漏洞评估能力，提供多种Web应用漏洞的安全检测，如“SQL注入、跨站脚本、文件包含、CSRF、目录遍历”等网站脆弱性漏洞。 |
| 1.
 | **主机漏洞扫描** | 集成多种POC对内网资产进行自动漏洞验证与渗透，发现可导致数据泄露、系统入侵、越权等可入侵漏洞，先于黑客发现此类漏洞，主动发现。 |
|  | 支持各类应用资产的弱口令扫描，可扫描的应用包括“SSH\SMB\RDP\TELNET\FTP\POP3\VNC\SNMP\VMAUTHD\POSTGRES\MSSQL\MYSQL\ORACLE”支持自定义字典，支持设置弱口令扫描白名单，可以指定某个ip某个应用不执行弱口令扫描。 |
|  | **主机漏洞管理** | 支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注。 |
|  | **大屏展示** | ▲具备资产风险趋势大屏，大屏内容包括资产概况、资产列表、资产类型、高危端口数量分布、脆弱性分布、资产风险排行、高危端口数、基线核查、主机漏洞、弱口令。资产概况，资产概况包括设备总数以及在线率、在线数和离线数；资产列表，包括中间件、操作系统、应用、厂商等；资产类型，包括主机、物联网设备等；资产信息展示包括资产名称、IP地址、设备类型、所属部门、资产状态；脆弱性分布，包括可入侵漏洞、数量等；高危端口数量分布；资产风险排行。**（提供功能截图证明）** |
|  | 具备漏洞风险趋势大屏，大屏内容包括主机漏洞、WEB漏洞、弱口令类型统计；漏洞展示细粒度包括发现时间、资产IP、漏洞名称、漏洞等级以及漏洞类型。同时可以对风险主机、风险网站、弱口令进行TOP展示，方便安全服务人员分析。 |
|  | ▲具备安全检查趋势大屏，大屏内容包括等级保护、个人信息保护、数据安全、国密合规、三甲评审、电子病历评级、互联互通评级、智慧医院评级、互联网诊疗、网络安全任务书的成熟度评估分数展示。**（提供功能截图证明）** |
|  | **配置核查** | 支持20种以上常见设备和应用的配置检查，包括操作系统、应用中间件、数据库。 |
|  | 操作系统类型，支持Windows2003/2008/2012/2016/2019/7/8/10/11；支持linux（Centos、Redhat、suse等）；应用服务，支持Linux、Windows下的Apache、Weblogic、TOMCAT、Websphere、Nginx，以及windows2003/2008/2012/下IIS6/7/8；数据库，支持Linux、Windows下Oracle8i/9i/10/11g、Mysql。 |
|  | **等级保护****2.0** | 支持无限制系统数量等保2.0标准二级、三级差距分析、自动评分及完成度比例模型展示。 |
|  | ▲提供一站式等级保护差距量化评估服务，等级测评介绍包括等级划分、等保整体流程图、测评指标；测评概况包括等级检测概况、等级检测列表，等级检测列表可清晰展示医院等级保护检测任务详细情况，如每个检查任务的名称、检查次数、等级、符合情况（符合、部分符合、不符合、不适用）、分数、检测时间。**（提供功能截图证明）** |
|  | 支持无限制数量新系统上线自动化安全测评及等保自评分 |
|  | ▲支持检测任务下钻，支持等级保护技术要求概况展示，包括安全物理环境、安全通信环境、安全区域边界、安全计算环境、安全管理中心，以符合、部分符合、不符合、不适用四个维度展示，协助用户了解等保技术要求符合概况。支持等级保护管理要求概况展示，包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理，以符合、部分符合、不符合、不适用四个维度展示，协助用户了解等保管理要求符合概况。**（提供功能截图证明）** |
|  | **个人信息保护** | 支持个人信息保护差距分析、自动评分及完成度比例模型展示。 |
|  | ▲支持个人信息保护评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用；检测维度包含个人隐私保护职责及岗位设置、个人隐私保护制度体系、个人信息的收集、个人信息存储、个人信息的使用、个人信息主体的权利、个人信息的委托处理共享转让公开披露。**（提供功能截图证明）** |
|  | **数据安全** | 支持数据安全差距分析、自动评分及完成度比例模型展示 |
|  | ▲支持数据安全评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用；检测详细内容包含数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁，涵盖数据安全全生命周期。**（提供功能截图证明）** |
|  | **国密合规** | 支持国密合规安全差距分析、自动评分及完成度比例模型展示 |
|  | 支持国密合规评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用；检测维度包含物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置。**（提供功能截图证明）** |
|  | **三甲评审** | 支持医院三甲评审安全差距分析、自动评分及完成度比例模型展示。支持医院三甲评审安全评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用；检测详细内容包括要求项、得分、检测结果、人工修改、操作。**（提供功能截图证明）** |
|  | **电子病历评级** | 支持医院电子病历评级安全差距分析、自动评分及完成度比例模型展示。 |
|  | ▲具备医院电子病历评级安全评估能力，协助医院通过电子病历测评。包括：支持电子病历评级安全评估模块，对医院电子病历评级安全评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用。检测维度包括：1、未形成电子病历。2、独立医疗信息系统建立。3、医疗信息部门内部交换。4、部门间数据交换。5、全院信息共享，初级医疗决策支持。6、统一数据管理，中级医疗决策支持。7、全流程医疗数据闭环管理，高级医疗决策支持。检测详细内容包括要求项、得分、检测结果、人工修改、操作。**（提供功能截图证明）** |
|  | **智慧医院评级** | 支持医院智慧医院评级安全差距分析、自动评分及完成度比例模型展示 |
|  | 支持智慧医院评分任务下钻，任务详情可查看检测概况，维度包括符合、部分符合、不符合、不适用；检测详细内容包括要求项、得分、检测结果、人工修改、操作。**（提供功能截图证明）** |
|  | **互联互通评级** | 支持互联互通评级安全差距分析、自动评分及完成度比例模型展示。 |
|  | ▲支持互联互通安全评估能力，协助医院通过互联互通测评。包括：支持互联互通评级模块，对医院互联互通评级安全评分任务下钻，任务详情查看可统览检测概况，维度包括符合、部分符合、不符合、不适用；检测维度包括硬件基础设施建设、网络及网络安全情况、信息安全情况。检测详细内容包括要求项、得分、检测结果、人工修改、操作。**（提供功能截图证明）** |
|  | **安服流程管理** | ▲支持对安服流程进行全生命周期管理，包括服务阶段计划、安全服务任务1、安全服务进度、安全工作提醒、安全服务报告、安全服务完成率。其中安全服务内容涵盖资产发现梳理、漏洞扫描、基线配置核查、安全加固、渗透测试、新系统上线安全评估、钓鱼邮件测试、应急响应、应急演练、安全培训、小程序公众号应用安全评估等。**（提供功能截图证明）** |
|  | **安全运营知识库** | 内置等级保护2.0、个人信息保护、数据安全、国密安全等安全制度及操作规程，安全制度及操作规程总数不低于1000+。内置安全法律法规、安全培训、应急处置、故障处置等安全运营文件。 |

## ★实施人员配置（须提供承诺书及近6个月任意一个月的社保证明）

供应商需提供3名及以上的实施团队保障该项目实施、培训及上线、免费顾问咨询等工作，在项目周期内，若采购人要求增派人员，供应商应全力配合采购人，按照甲方要求进行人员增派。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **岗位** | **人员数量** | **岗位工作内容** | **备注** |
| 1 | 项目经理 | 1 | 管理项目整体进度、按照招标方要求进行需求沟通 | 3年相关行业工作经验 |
| 2 | 实施工程师 | 1 | 对项目需求进行落地实施 | 2年相关行业工作经验 |
| 3 | 安全服务工程师 | 1 | 提供网络安全等级保护测评整改相关安全服务，如协助相关系统的操作系统主机配置加固、对主机漏洞进行扫描及修复等。 | 2年相关行业工作经验 |

# 其他要求

## 安全保密要求

1）确保遵守江门市第二人民医院的保密规定，并签订保密协议，且保密责任不因合同的中止或解除而失效。

2）未经业主管理人员的许可不得将各种带有信息的介质带出单位。

3）未经业主管理人员的许可不得进入中心机房操作，进入中心机房操作须遵守机房管理规定。

4）未经业主管理人员的许可不得进入江门市第二人民医院信息系统查看、复制、增加、删改信息和数据。

## 实施要求

### 服务实施要求

供应商须提供以下承诺：

（1）供应商提供的截图、资质等证明文件应真实有效；

（2）供应商应对了解到的信息保密，保密要求按照需求书

（3）在江门市第二人民医院进行整改过程中提供必要的技术支持；

（4）能按照江门市第二人民医院规定的工作内容及进度安排协助完成等级保护工作；

（5）项目必须按照国家网络安全等级保护的标准要求开展。

★（6）实施时间：必须在合同签订后，于2025年12月30日前完成对应系统的等级保护评测工作，并取得对应回执或者证书。

### 项目组织管理要求

本项目需配备专业的实施团队负责本次项目的具体实施工作，团队应配备专业项目经理、实施人员等项目所需各类角色人员负责项目实施。项目实施工作人员保持相对稳定，投标人应书面明确实施投标项目的人员配置管理计划，包括组织结构、项目负责人、组成人员的资历信息、类似项目的经验及分工职责。

### 计划与进度管理要求

投标人须在投标文件中针对本项目采购需求制定工作方案，明确招标项目工作的方式、方法、过程步骤、按阶段分解的详细计划、对应计划应提交的工作成果、需要采购人协调与配合的事项。

## 项目工期要求

合同签订后，于2025年12月30日前完成对应系统的等级保护评测工作，并取得对应回执或者证书。

## 验收要求

本项目合同签订后每年完成采购方要求测评的系统等级保护评测工作。

项目整体测评完成后并由中标人向采购方提出项目验收申请，采购方组织相关人员与中标人一起进行整个项目的验收工作。

验收内容和验收标准参照既定的技术方案、实施要求和验收标准。

(1) 验收原则：项目整体测评完成后验收。

(2) 验收时间：当安全等级评测及问题整改完成无后续问题发生，经专家复审备案通过后，由中标人向采购方提出项目验收申请单，采购方在收到中标人提交的验收申请单的 15 天内，组织相关人员与中标人一起进行项目的验收工作，在验收过程中中标人需要出具相关的盖章报告。

(3) 验收内容和验收标准参照既定的技术方案、实施要求和验收标准。

①本合同规定的工作内容；

②合同附件；

③用户需求书；

④其 他: 。

4、验收小组成员：采购人应组织相应的信息科技术人员、使用该系统的科室、职能科室或院外专家，形成验收小组，供应商技术

人员作为验收材料汇报方；在验收小组组长的主持下，对项目进行验收。

5、验收方式：

本合同项目得到采购人认可后，按照本合同要求，供应商工程实施人员将向采购人提出验收请求并提交《实施验收申请单》，采购人应在收到供应商实施人员提交的验收申请后，依据验收标准，验收小组逐项检验、测试，当系统达到验收标准后，以采购人的信息科及使用部门与供应商 共同签署验收报告为验收合格。 验收合格后，双方授权代表应共同签署书面报告。验收报告签字之日为软件系 统验收合格日期。如验收不合格，供应商应提供书面的整改方案并立即实施补救，直到满足本合同定义的验收标准中的全部内 容。补救工作应在双方协定的工作日内完成，整改完成后无故障运行一个月，双方再次组织验收，合格后以书面予以确认。

 6、交付文档验收标准：

对于本次项目所涉及的文档项目的工作内容及成果覆盖以下内容的电子文档：包括但不限于以下部分。实施进场申请函、启动报告、项目实施计划(里程碑)、用户文档(包括：安装手册、操作手册、维护手册)、用户培训记录、《\*\*\*\*系统安全等级测评报告》、漏洞扫描报告、《安全问题整改清单》、项目实施过程中衍生的其它相关资料。

## 售后服务要求

本次项目中提供的产品及系统平台须至少提供3年质保服务。

在提供的产品及系统平台维护期内，投标人要提供客户服务热线及完善的响应机制。

对提供的产品及系统平台提供包括（但不限于）系统维护、错误修正在内的全方位免费维保服务。维护期内投标人因维护所发生的一切费用均由投标人承担。

投标人须制定详细服务计划，每季度对系统进行漏洞检查、安全监测及其他服务，防止系统发生故障。

免费维保服务期满后终身有偿保修，属于免费维保服务期届满后的有偿维保服务期内并且不属于中标人所供货物或服务质量问题的事项，中标人每年可收取不超过中标金额8%的维护费，费用由采购人承担，中标人仍需及时修复并交采购人验收合格后继续使用。

## 培训要求

培训目标要求

培训目标是使参加项目相关的各级领导、业务人员、项目管理人员和技术人员得到相应的培训，以便在软件及设备部署、软件及设备管理、运行维护等各个阶段都具有相应的具有科学素养的人才保障实现预期目标。

培训的对象要求

主要面向江门市第二人民医院的信息化技术人员，包括但不限于机房维护人员、系统维护人员等。

培训内容要求

（1）产品使用培训要求

针对本次项目中的所有产品，包括但不限于安全设备、网络设备，为了在部署后得到充分利用，投标人需要对江门市第二人民医院的信息化技术人员进行操作技能、系统功能、网络安全和相关基础知识等方面的培训，以加强操作人员对系统的了解和掌握，提高使用效率。

# 评审方法

## 评标方法

**本项目采用综合评分法**。评标委员会对符合性审查合格的投标文件进行商务、技术和价格评审，如有多个包组则按各包组的自然顺序进行评审。评标委员会的评审以招标文件为依据按照评标程序，就每个投标人的商务状况、技术状况及其对招标文件要求的响应情况进行评审和比较，独立评出各投标人的商务得分、技术得分。各评委的评分算术平均值即为该投标人的商务得分和技术得分；然后评出价格得分；最后将商务得分、技术得分和价格得分汇总得出综合得分（商务得分、技术得分、价格得分分值按四舍五入原则精确到小数点后两位）。

**综合得分＝商务得分+技术得分+价格得分**

1. 商务、技术评分

评标委员会对投标人的商务、技术状况及响应程度进行评议和比较，并依据评分标准，评出其商务、技术评分。【详细评分标准见《详细评审表》】

1. 价格评分

价格评分采用低价优先法计算，即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，其价格分为满分，落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价，【详细评分标准见《详细评审表》】其他投标人的价格分统一按照下列公式计算：

**价格得分=（评标基准价/投标报价）×价格权重×100**

## 评分权重分配表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **评分项目** | **商务评分** | **技术评分** | **价格评分** | **合 计** |
| **权重** | **20%** | **70%** | **10%** | **100%** |
| **分值** | **20分** | **70分** | **10分** | **100分** |

## 详细评审表

|  |  |
| --- | --- |
| **评审因素** | **评审标准** |
| **分值构成** | 技术部分70.0分商务部分20.0分价格部分10.0分 |
|  | **评分因素** | **分值** | **评分准则** |
| **技术部分（70.0分）** | **项目技术方案** | 10 | 内容完整、详细、表述清晰、科学合理、切实可行，得7-10分；内容比较完整、详细、表述清晰、比较合理、可行，得3-7分；内容基本完整、详细、表述基本清晰、合理、可行性稍差，得1-3分；其他或无响应，得0分。 |
| **项目实施方案** | 10 | 内容完整、详细、表述清晰、科学合理、切实可行，得7-10分；内容比较完整、详细、表述清晰、比较合理、可行，得3-7分；内容基本完整、详细、表述基本清晰、合理、可行性稍差，得1-3分；其他或无响应，得0分。 |
| **质量保证方案** | 10 | 内容完整、详细、表述清晰、科学合理、切实可行，得7-10分；内容比较完整、详细、表述清晰、比较合理、可行，得3-7分；内容基本完整、详细、表述基本清晰、合理、可行性稍差，得1-3分；其他或无响应，得0分。 |
| **安全服务工具技术指标要求响应情况** | 40 | 根据项目采购文件内容要求，完全满足或优于采购文件“安全服务工具要求”，全部满足得40分，每项▲指标项不满足或部分满足扣2分，其他指标项不满足或部分满足扣1分，扣完为止。如有要求提供产品截图或检测报告的指标项，必须提供证明文件，否则响应无效。 |
| **商务部分（20.0分）** | **同类业绩经验** | 5 | 要求投标人具有医院安全服务相关项目案例，每提供一个得1分；累计得分最高不超过5分。注：须提供自2022年1月1日以来合同关键页（含签订合同双方的单位名称、合同项目名称、采购内容、签订合同双方的落款盖章、签订日期）的扫描件加盖投标人公章，不提供相关证明资料，不得分。 |
| **项目经理要求** | 2 | 投入本项目的项目经理，具备以下证书：1、具有本科或以上学历证书。2、具有“计算机技术与软件专业技术资格（水平）考试”信息系统项目管理师证书。每提供一个证书得1分，满分为2分。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。 |
| **项目实施团队要求** | 4 | 投入本项目的项目团队成员（不包括项目经理）2名或以上：项目团队成员（不包括项目经理）至少2人具有信息安全保障人员证书（覆盖安全运维、安全集成、应急服务、风险管理4个安全方向），每提供1人得2分，满分4分。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。 |
| **企业资质情况** | 9 | 投标人具有由国家认证认可监督管理部门批准设立的认证机构颁发并在有效期内的以下证书，总分最高得9分。（1）具有质量管理体系认证证书，得1分；（2）具有环境管理体系认证证书，得1分；（3）具有职业健康安全管理体系认证证书，得1分；（4）具有信息安全管理体系认证证书，得1分；（5）具有信息技术服务管理体系认证证书，得1分；（6）具有信息安全服务资质认证证书（安全集成、应急处理、风险评估、安全运维），每提供一种服务资质得1分，最高得4分。注：须提供有效证书复印件及国家认证认可监督管理委员会官方网站（http://www.cnca.gov.cn/）有效查询的信息截图，加盖投标人公章。 |
| **价格部分（10.0分）** | **投标报价** | 10 | 投标报价得分＝（评标基准价/投标报价）×价格分值【注：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。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。 |