**附件1**

**江门市妇幼保健院2025年信息系统等级保护测评项目采购需求**

# 总体要求

1. 供应商需出具承诺函，承诺结合《风险梳理整改建议》协助及参与医院开展全面的整改工作，直至系统通过等级保护测评（格式自订）；

2. 供应商需出具承诺函，承诺2025年内完成信息系统等级测评,并将最终的《信息系统等级测评报告》提交至江门市公安局网安支队进行备案（格式自订）；

3、响应供应商应保证，采购人在中华人民共和国使用该服务或服务的任何一部分时，免受第三方提出的侵犯其专利权、商标权、著作权或其它知识产权的起诉。

# 投标报价说明

报价方式为广东省江门市目的地交付验收价，均涵盖报价要求之一切费用。报价中必须包含完成所有等级保护综合服务及合同条款所规定的工作内容的各项费用，应包括人工、设备、工具、项目管理、场地踏勘、维护服务、利润、税金、合同实施过程中的应预见和不可预见费用等，报价中漏报、少报的费用，视为此项费用已隐含在响应报价中，成交后不得再向采购人收取任何费用。

# 项目需求

## 项目概况

随着信息化程度的越来越普及，而且国内外信息安全形式非常严峻，结合国家信息安全等级保护的安全要求，同时根据《网络安全法》及相关网络安全文件的要求，为保障所有服务器系统和各类应用系统的安全稳定运行，同时响应公安部门提出的进行信息系统安全等级保护建设工作的要求，拟通过第三方专业安全公司提供先进的、专业的安全服务，对整体系统进行全面、动态的等保合规综合服务工作，时刻保障业务系统信息安全。

## 项目服务范围

1.、项目系统清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **测评级别** | **内外网** |
| 1 | 妇幼保健信息系统平台 | 三级 | 专网 |
| 2 | 互联网医院系统平台 | 三级 | 外网 |
| 3 | 医院管理信息系统 | 三级 | 专网 |
| 4 | 集成平台 | 三级 | 内网 |

1. 安全整改：根据对目标系统进行风险梳理，提交《风险梳理整改建议》，结合《风险梳理整改建议》协助及参与医院开展全面的整改工作，直至系统通过等级保护测评【投标方需要提供系统通过的承诺函】。

3、安全托管服务：服务供应商需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新 。

## 项目目标

以等级保护标准为基础，通过系统性的安全服务，进一步建立完整的安全管理体系和动态的安全保障，通过前沿的合规加保障的服务，周期性地对单位的所有资产进行动态检测和动态保障，提高核心服务器群整体的安全性。

## 项目内容要求

### 资产梳理服务

对江门市妇幼保健院的资产进行梳理，建立江门市妇幼保健院有效安全资产管理，能以资产为安全管理单位进行有效的安全运维工作，并通过实时展示资产的安全风险指数。

1、网站资产梳理

对单位系统进行自动化梳理服务，能主动探测互联网上暴露的资产，形成明确的资产清单，发现未知资产，并发现直接对外开放的危险连接方式。

2、服务器资产梳理

对江门市妇幼保健院服务器进行自动化梳理服务，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等，实现对服务器的自动化运维管理。

3、终端资产梳理

对江门市妇幼保健院终端PC资产自动化梳理服务，对识别到的所有IP地址进行有效管理，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等。

### 安全隐患排查服务

安全隐患排查是实现网络安全管理的前提和基础，为了满足各业务系统的基本安全需求，就需要充分参考国家及行业标准、规范以及成熟经验，建立并形成一个针对各业务系统的安全模型。

服务单位使用安全隐患排查工具或人工检查，对江门市妇幼保健院管辖范围内网络设备、主机、操作系统、数据库、中间件、应用软件进行安全隐患核查及是否满足等保规范的原则进行配置，并提供相对应报告。

### 安全运维监测服务

**网站风险与威胁监测**

对1个网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等7个维度开展实时监测。

**主机漏洞扫描和漏洞管理**

通过可视化呈现服务工具平台，自动化探测主机、网站资产，可定位和识别主机操作系统、开放端口、应用服务、协议版本，子域名、url、web框架、备案号等，形成可动态管理的资产台账，可通过用户现有的资产台账导入结合，进行补充和更新。

**弱口令监测**

通过可视化呈现服务工具平台，自动化探测主机、网站资产“SSH、SMB、RDP、Telnet、Ftp、pop3、VNC、SNMP、Vmauthd、Postgres、MsSQL、MySQL、Oracle”存在的弱口令情况。

**互联网威胁诱捕**

通过部署威胁诱捕平台，基于欺骗防御技术，诱骗攻击者、病毒主机攻击蜜罐陷阱，实时零误报定位攻击威胁进行预警。

**边界威胁监测**

通过流量镜像对海量流量进行采集，基于40000+威胁特征库，对于捕获的流量进行存储、分析，内置多重检测引擎，包含入侵检测、web检测、威胁情报等，结合攻击源、风险等级、地理位置、攻击目标、命中规则数、告警次数等因素综合分析，精准识别攻击源头，发现不同场景下的已知威胁和未知威胁。

### 安全加固服务要求

根据安全隐患排查服务中的《问题整改清单》中提出的问题，在江门市妇幼保健院提供完整的网络安全加固服务，并指导江门市妇幼保健院的系统开发人员开展整改加固工作。主要包括：对问题清单中网络设备、安全设备、服务器的配置加固，推进江门市妇幼保健院的整改实施进度等相关工作，提供满足等级保护安全要求的安全设备协助江门市妇幼保健院通过等级保护测评。

根据《信息安全技术 网络安全等级保护基本要求》，对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面进行安全管理体系的完善，对目前不满足等级保护相关要求的安全管理制度进行补充、修订与编写，以达到满足《信息安全技术 网络安全等级保护基本要求》的目标。

### 等级保护测评要求

**定级备案**

根据《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》等标准，对本项目的信息系统进行调研，协助江门市妇幼保健院完成4个三级系统的《信息系统定级报告》编写工作、填写系统定级备案的相关资料及专家评审，完成定级备案工作，并向当地公安局备案，取得《网络安全等级保护备案证明》。

**等级测评**

准聘请具有网络安全等级测评与检测评估认证的测评机构组织对4个三级系统开展网络安全等级保护符合性测评，衡量江门市妇幼保健院信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备相应的安全保护能力。

依据信息系统的安全保护等级，通过人员访谈、文档查、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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面，判断信息系统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，组织专家评审，编写安全等级保护测评报告，最终完成验收测评工作，达到国家规定的信息安全要求，并完成向江门市公安局提交测评备案工作。

## 项目实施基本要求

（1）响应供应商提供的资格、资质等证明文件应真实有效，签订合同前江门市妇幼保健院有权核查这些证明文件的原件。

（2）成交供应商须保证对本项目实施中所获得任何资料和信息严格保密，并与江门市妇幼保健院签订保密责任书。

（3）成交供应商须按照江门市妇幼保健院规定的工作内容及进度安排完成项目工作。

## 交付报告要求

服务中产生的全部档案资料版权归江门市妇幼保健院所有，未经江门市妇幼保健院允许的情况下，不得以任何形式向第三方提供安全技术文档的全部或部分内容，交付文件包括但不限于如下成果和报告：

1. 项目实施方案
2. 资产梳理报告
3. 安全隐患排查报告
4. 月度安全综合服务报告
5. 安全加固报告
6. 定级备案材料
7. 网络安全等级保护测评报告
8. 其他江门市妇幼保健院认为有必要的交付物

## 安全保密要求

成交供应商应当与江门市妇幼保健院签署保密协议，对于安全服务所获取的相关信息进行严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据、信息进行任何侵害江门市妇幼保健院信息系统的行为。

# 商务要求

## 组织实施要求

1)应安排专职项目经理负责本次项目的实施。

2)应保证项目团队成员的稳定，以保证服务的质量和连贯性。

## 交付要求

本项目服务期限，2025年内完成上述服务内容，提交《资产梳理报告》、《安全隐患排查报告》、《季度安全综合服务报告》、《安全加固报告》《定级备案材料》并将最终的《信息系统等级测评报告》提交至江门市公安局网安支队进行备案。

## 整体技术要求

1）本项目中可能需要的硬件平台（如笔记本电脑、PC、工作站等）均由中标方提供，采购方将按照相关要求对设备进行必要处理。中标方在服务期间未经采购方许可不得将设备带离采购方指定场所，也不得使用任何未经采购方确认的存储设备对测评数据进行复制。

2）安全测评、评估等应按照分层的原则，包括但不限于以下对象：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、安全运维管理等。

3）中标方在服务过程中应尽可能小的影响系统和网络的正常运行，不能对系统的运行和业务的正常提供产生显著影响。

4）中标方应对服务工作中所产生的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，采购方有权要求在评估结束之后销毁所有和评估有关的数据和文档。

## 付款方式

付款方式：经甲方验收合格后20个工作日内申请支付合同全款金额。