

# 广东医科大学顺德妇女儿童医院

## 2023 年三级信息系统等级保护评测项目需求书

1 项目名称：信息系统三级等保评测（7 个系统）

2 项目预算：55.3 万元

3 项目总体概要

### 3.1 项目概述

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《信息安全等级保护管理办法》与佛山相关网络信息安全文件的要求，我单位计划对已定级测评的三级信息系统进行信息安全等级保护测评工作。

### 3.2 货物一览表

序号	项目	说明	单位	数量	备注
1	信息系统三级等保评测（7 个系统）	详见以下指标要求	项	1	新购
2	集成整改服务	详见以下指标要求	项	1	新购

### 3.3 服务要求

通过对信息系统的信息安全等级保护情况进行风险梳理、目前的安全状况和存在的安全风险程度，出具相应的整改建议清单，以推动信息系统等级保护制度的有效落实。

根据《GB/T 22239—2008 信息安全技术信息系统安全等级保护基本要求》等标准组织开展广东医科大学顺德妇女儿童医院信息系统等级保护符合性测评，衡量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，是否具备了相应的安全保护能力，提交《网络安全等级保护测评报告》。

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、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。

### 3.4 详细技术参数要求

说明：带“▲”号条款为评审时的重要技术参数，不作为投标无效条款。如中标后缺少整体架构所必需部件，均由中标方免费提供。

#### 3.4.1 ▲信息系统三级等保评测（7 个系统）

➤ 需测评系统清单：

序号	系统名称	系统等级	备注
----	------	------	----

1	HIS 系统	三级	年测
2	互联网医院系统	三级	年测
3	住院电子病历系统	三级	年测
4	医院信息集成平台	三级	年测
5	OA 系统	三级	年测
6	LIS 系统	三级	年测
7	PACS 系统	三级	年测

供应商需协助采购人完成以上 7 个信息系统的等保测评相关流程工作，具体工作包含：

1、收集用户系统相关信息（资产清单、接口人、系统描述），联系测评机构。

★2、本期项目实施工期不得超过 90 个工作日，供应商需保证在规定的时间内协助用户通过等保测评，并且拿到《网络安全等级保护等级测评报告》。

2、协助用户进行定级备案材料编写，如信息系统等级保护备案表，信息系统等保保护定级报告等。

3、配合测评机构，梳理测评过程和收集测评对象相关信息。

4、对于测评过程中发现的高风险项问题，及时与客户汇报沟通。

5、协调测评机构编写报告。

### 3.4.2 ★集成整改服务 1 项

1、供应商依据《信息系统安全等级保护测评要求》对本单位的信息系统安全等级保护状况评估，包括以下两个方面的内容：

（1）安全技术评估，主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个层面上的测评；

（2）安全管理评估，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、安全运维管理评估。

若判定系统安全防护能力无法达到相应级别或要求，则提交《整改问题清单》。

2、供应商根据《整改问题清单》，提供技术手段协助用户进行安全整改。

3、参照《差距测评问题清单》协助甲方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。其中整改服务包括但不限于：

#### （1）服务器安全加固服务

服务器操作系统的身份鉴别安全加固，配置登陆失败、操作超时、限制非法登录以及自动退出等；

配置服务器账号登录密码强度策略；

严格控制服务器操作系统的远程管理，限制远程管理终端，配置使用加密远程管理方式等；

对服务器操作系统账号的权限进行紧缩，遵循“最小权限”原则，防止对系统的越权访问；

清理不再使用、旧的系统账号；

禁用系统多余的、系统缺省打开却不必要服务系统服务，删除不再使用的共享；

开启系统日志审计功能，对系统事件的日期、时间、类型、主体标识、客体标识等进行记录，并定期分析；

配置服务器操作系统的防病毒及防恶意代码功能，安装防病毒软件，定期进行病毒查杀；

检查分析现有系统的安全漏洞和黑客后门等，更新服务器系统安全补丁；

对服务器操作系统的运行状态、系统服务等进行监控；

配置应用平台（IIS、apache 等）的安全参数，加强应用安全。

#### （2）关键网络设备加固

根据相关策略对设备进行检查与设置，并进行优化调整；

对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，启用路由器中的 ACL 配置，提高接入的安全性等措施优化配置，实现设备加固。

#### （3）安全设备加固

根据相关策略对设备进行检查与设置，并进行优化调整。

对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，提高接入的安全性等措施优化配置，实现设备加固。

4、在信息系统完成风险梳理和整改实施之后，供应商需要再次通过测评手段对信息系统的安全技术和安全管理上各个层面的安全控制进行整体性验证，提供的验收测评服务将协助本单位完成等级保护测评工作，对信息系统的安全等级保护情况及整改情况进行评审，出具《网络安全等级保护等级测评报告》。

#### 4 项目商务部分

评分内容	技术部分	商务部分	价格部分
权重	40%	30%	30%

##### 4.1 技术部分（权重 40%）

序号	评审因素	评分标准	分值
1	项目总体设计方案方案响应情况	<p>投标人需提供项目整体建设方案，从采购人视角出发，对平台建设总体架构和要点把握准确，系统总体设计方案从技术路线、技术架构、功能架构等方面综合考虑，思路清晰，并充分考虑系统的针对性、合理性、实用性、兼容性和功能完备性等。</p> <p>1、整体方案先进、合理、完整，技术路线把握精准、技术和功能架构完整先进，设计思路清晰，充分满足需求的，得 7 分；</p> <p>2、整体方案一般，技术路线把握不够精准，技术和功能架构保守，设计思路不够清晰，基本满足需求的，得 5 分；</p> <p>3、整体方案不合理，技术路线错误，技术和功能架构落后，设计思路模糊，不能满足需求的，得 3 分；</p> <p>4、其他或无响应的，得 0 分。</p>	7
2	核心技术响应程度	<p>根据投标人对采购需求中条款的响应程度进行评审：</p> <p>（1）完全满足且优于采购需求，得 6 分；</p> <p>（2）完全满足采购需求，得 4 分；</p> <p>（3）不完全满足采购需求，得 1 分。</p>	6
3	应急响应方案	<p>（1）应急方案针对性强、可行性强，7 分；</p> <p>（2）应急方案针对性、可行性较强，4 分；</p> <p>（3）应急方案不完整或可行性一般，1 分；</p> <p>（4）没有提供方案的得 0 分。</p>	7
4	投标人拟派项目经理经验及资质能力水平情况	<p>1、具有信息系统项目管理师认证证书；</p> <p>2、具有 Oracle 数据库原厂 OCP 认证证书；</p> <p>3、具有容灾实施专家认证；</p> <p>4、具有信息安全保障人员认证证书和 ITSS IT 服务工程师证书；</p> <p>5、具有 RHCE 认证证书；</p> <p>6 具有项目管理专业人员资格认证（PMP 认证）；</p> <p>项目经理同时具备以上 6 个得 16 分，一项不满足扣 3 分，扣完为止。注：投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月内任意月份的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。</p>	16

5	项目实施团队能力	<p>1、实施团队中有注册信息安全工程师不少于 2 人。</p> <p>2、实施团队中有人社局颁发的网络工程师中级或以上认证不少于 1 人。</p> <p>3、实施团队有 1 人及以上通过 VMware 虚拟化软件官方认证的专业技术人员。</p> <p>4、实施团队中技术人员（提供有效期内的专业资格认证证明）至少 1 名通过高级信息系统项目管理师认证的专业技术人员。</p> <p>投标人根据项目实施团队情况提供上述认证，同时具备以上 4 个得 4 分，一项不满足扣 2 分，扣完为止。</p> <p>注：投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前 1 个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。</p>	4
合计			40 分

#### 4.2 商务部分（权重 30%）

序号	评审因素	评分标准	分值
1	投标人管理体系	<p>1、具有 ISO9001 质量管理体系认证；</p> <p>2、具有 ISO27001 信息安全管理体系统认证；</p> <p>3、具有 ISO14001 环境管理体系认证；</p> <p>4、具有 ISO20000 IT 服务管理体系认证；</p> <p>5、具有知识产权管理体系认证证书；</p> <p>投标人具有上述 5 项认证，一个认证得 2 分，满分得 10 分，不满足不得分；</p> <p>注：1. 提供与投标人名称一致的有效的质量认证证明文件复印件，并加盖投标人公章；2. 上述证书的发证机构须为境内机构；否则不得分）</p>	10
2	投标人服务能力	<p>1、具有 ITSS 数据中心服务能力成熟度标准符合性证书二级和具有 ITSS 信息技术服务运行维护服务能力成熟度模型，满足得 2 分，不满足不得分；</p> <p>2、具有信息系统建设和服务能力等级证书满足得 2 分，不满足不得分；</p>	17

		<p>3、具有 CMMI 能力成熟度模型证书，满足得 2 分，不满足不得分；</p> <p>4、具有数据库安全相关的软件著作权，每具有一个得 0.5 分，最高 2 分；</p> <p>5、具有中国网络安全审查技术与认证中心 CCRC 颁发的信息安全服务资质-认证方向为信息系统安全集成、安全运维服务、信息安全风险评估证书。每个得 2 分，满分 6 分；</p> <p>6、具有计算机信息系统安全服务等级证书，满足得 3 分，不满足不得分；</p>	
3	类似项目经验	<p>投标人 2019 年以来完成的医疗行业安全运维整改相关项目实施经验，每个得 1 分，最高得 3 分；</p> <p>（提供合同复印件及合同发票作为评审依据，否则有可能影响评审结果）。</p>	3
合计			30 分

#### 4.3 价格部分（权重 30%）

经评选小组审核，满足采购文件要求，以折扣率最低者定为评选基准价，其对应报价得分为满分。

报价得分 = (评选基准价 ÷ 评选最后报价) × 价格分值

#### 5 付款方式

合同签订后 15 个工作日内，凭投标人提供的等额发票，招标人按合同总价的 50% 向投标人支付首付款。

投标人出具本项目的问题清单后，经招标人组织验收合格后 15 个工作日内，凭投标人提供的等额发票，招标人向投标人支付合同总价的 30%。

投标人出具测评报告后，经招标人组织验收合格后 15 个工作日内，凭投标人提供的等额发票，支付尾款 20%。