**浙江大学医学院附属儿童医院**

**2023年信息安全等级保护测评项目**

**1、项目概况**

为贯彻落实国家信息安全等级保护制度，浙江大学医学院附属儿童医院决定对本单位开展信息安全等级保护测评工作，并进一步完善浙江大学医学院附属儿童医院的信息系统安全管理体系和技术防护体系，切实提高浙江大学医学院附属儿童医院系统信息安全防护能力。

依据国家信息安全等级保护相关标准及技术规范要求，结合浙江大学医学院附属儿童医院信息安全整体需求及各系统具体应用特点，对浙江大学医学院附属儿童医院指定相关信息系统开展安全测评，出具信息安全等保测评报告，并协助完成系统定级备案。

**2、项目采购内容及数量**

本项目等级测评服务包括但不仅限于以下内容：

对浙江大学医学院附属儿童医院的6个信息系统进行等级保护测评（系统列表如下），并协助浙江大学医学院附属儿童医院开展此次测评系统的定级备案工作。

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 系统等级 |
| 1 | 浙大儿院APP | 三级 |
| 2 | 浙江大学医学院附属儿童医院基础支撑系统 | 三级 |
| 3 | 浙江大学医学院附属儿童医院面向患者服务系统 | 三级 |
| 4 | 浙大儿院集成平台系统 | 三级 |
| 5 | 门户网站系统 | 二级 |
| 6 | 浙江大学医学院附属儿童医院办公系统 | 二级 |

**3.项目标准：**

安全等保测评应依据但不限于以下国家信息安全标准：

《浙江省信息安全等级保护管理办法》（省政府223号令）

GB/T 22239-2019：《信息安全技术 信息系统安全等级保护基本要求》

GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

GB/T 25058-2010：《信息安全技术 信息系统安全等级保护实施指南》

GB/T 28448-2019：《信息安全技术 信息系统安全等级保护测评要求》

GB/T 28449-2018：《信息安全技术 信息系统安全等级保护测评过程指南》

**4.技术要求**

**4.1.定级要求**

实施方应依据《信息系统安全等级保护定级指南》要求协助采购单位完成首次测评的信息系统定级备案工作，并编制信息系统《等级保护定级报告》和《备案表》等相关内容。

**4.2.测评内容**

根据采购单位信息系统的安全保护等级，并依据《GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求》、GB/T 28448-2019：《信息安全技术 信息系统安全等级保护测评要求》的条款要求，逐一对信息系统的安全保护等级进行测评，包括但不限于以下内容及要求：

1、安全技术测评：包括安全物理环境、安全区域边界、安全计算环境、安全通信网络、安全管理中心五个方面的安全测评；

2、安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

**4.3.测评原则**

本次安全保护等级保护测评实施方案设计与具体实施应满足以下原则：

1、标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

2、规范性原则：实施方的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

3、可控性原则：测评服务的进度要跟上进度表的安排，保证采购方对于测评工作的可控性。

4、整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

5、最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

实施方应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

**4.4.测评要求**

1、实施方应在对采购方系统详细了解的基础上，编制针对性的等级保护测评整体实施方案，包括项目概述、等保测评范围和内容、项目实施流程、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

2、实施方应详细描述测评人员的组成、资质及各自职责的划分。配置有经验的测评人员进行本次等级保护测评工作。

3、本次等级保护测评实施过程中所使用到的各种工具软件由实施方推荐，经采购方确认后由实施方提供并在测评中使用。在投标文件中应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

4、对于在测评过程中采用的测评方法、测评所使用的工具、测评所覆盖的各方面，需要符合信息安全等级保护主管部门要求，包括但不仅仅包括网络隐患检测工具、数据库漏洞检测工具、应用安全检测工具、网站安全检测工具等。

5、实施方应详细描述需要的运行环境的具体要求。

6、项目完成后必须提交完整的技术文档、测评报告、整改建议等。

**4.5.项目实施要求**

1、实施方应保证投标项目在采购方条件成熟时应立即开展实施；

2、实施方在项目实施过程中应服从采购方的统一领导和协调，采购方有权裁决实施方的责任范围，实施方必须执行，在采购方限定的时间内解决问题。如果实施方不能按时完成测评内容，采购方有权中止项目、索赔或拒付款项；

3、实施方需根据自己的工程实施经验结合采购方的实际需求进一步细化和完善工作任务书，作为工程实施的指导性文件；

4、实施方应根据采购方工作需求、进度要求、实际情况制定详细的项目实施管理规范和项目实施计划，对工程目标、工作任务、阶段性工作、项目组织机构、职责分工、项目进度、质量控制等内容进行详细的说明，以确保工程实施按时保质的完成；

5、 实施方需为浙江省内服务单位，具有网络安全等级测评与检测评估机构服务认证证书，具有中国网络安全审查技术与认证中心颁发的信息系统安全运维二级服务资质认证证书（若中标，则应提供上述证明材料）。

6、本次项目实施骨干人员至少包含1名高级测评师（提供证书复印件）。本项目负责人必须具有高级测评师且同时具备CNLAB实验室认可的内审员证书以及注册信息安全专业人员CISP证书。项目参与人员应具有注册网络安全持有人已参加渗透评估专业人员(NSATP-A高级)、信息安全保障人员认证证书(CISAW)、系统集成项目管理工程师（中级）证书确保项目的顺利实施。

**4.6.项目验收**

实施方应在测评工作结束后，协助委托方完成系统的备案工作。服务完成后经用户验收合格支付合同金额。

本项目输出包括但不限于以下成果：

1. 《网络安全等级保护测评报告》
2. 《网络安全整改建议书》
3. 《信息系统安全等级保护备案证明》

**4.7.保密要求**

实施方应对项目实施过程中获取的信息系统重要数据采取严格的保密措施，防止数据泄露。

**5.商务要求**

|  |  |
| --- | --- |
| 售后服务 | 1.具体实施响应要求：如有技术疑难问题，须半小时内响应；如需到达现场处置，须2小时内到达2.技术咨询要求：在服务期内，提供信息安全的咨询服务，能够协助用户进行信息安全整改、制度建设等工作 |
| 服务时间及地点 | 服务地点：用户指定地点。服务期：合同签订后六十个工作日内完成，并出具测评报告。 |
| 履约保证金 | 无 |
| 付款条件 | 项目验收合格后凭有效票据60个工作日内付全款。 |