**南京大学医学院附属苏州医院**

**等级保护测评服务采购需求**

南京大学医学院附属苏州医院（苏州科技城医院）拟对等保测评项目组织院内调研，现欢迎符合相关条件的供应商参加本次采购活动。

一、项目编号：

二、项目名称：苏州科技城医院等保测评

三、项目预算：贰拾玖万元整（￥290000.00元）

四、最高限价：贰拾玖万元整（￥290000.00元）

五、合同履行期限: 自合同签订之日起一年

六、采购内容：

（一）项目背景

根据公安部关于开展重要信息系统和重点网站安全执法检查的工作要求，为更好的贯彻落实中央关于网络安全的重要指示精神，有效应对当前苏州科技城医院网络安全面临的严峻威胁与挑战，全力做好苏州科技城医院重要信息系统网络安全保卫工作，亟需对苏州科技城医院的核心系统展开等保评测与安全服务工作，通过该评测工作及时发现系统安全隐患并迅速进行整改，从而全面提升苏州科技城医院重要信息系统的网络安全防护水平，保障系统的安全、高效、稳定运行。

（二）项目原则

1.客观性和公正性原则：测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案开展。

2.保密原则：在测评过程中，需严格遵循保密原则，双方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购方利益。

3.最小影响原则：测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

4.规范性原则：信息安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

5.质量保障原则：在整个测评过程中，须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

6.系统安全原则：项目工作人员需遵守等保检测规定，采用符合标准的检测工具和检测方法实施检测，如因违规操作造成对检测系统的破坏，则应承担相应责任。

7.测评师规范原则：检测实施方工作人员必须通过公安部的等级保护等级测评师认证，持证上岗，经项目委托方确认资格后方可实施检测。

（三）项目依据

《中华人民共和国网络安全法》

《关于加强党政机关计算机信息系统安全和保密管理的若干规定》

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

《信息安全等级保护管理办法》(公通字[2007]43号)

《信息系统安全保护等级定级指南》（GB/T 22240-2008）

《网络安全等级保护基本要求》（GB/T 22239-2019）

《网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《网络安全等级保护测评要求》（GB/T 28448-2019）

《网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息系统安全管理测评》（GA/T 713-2007）

《信息安全等级保护等级测评实施细则》

《信息安全风险评估规范》（GB/T 20984-2007）

《信息安全风险管理指南》（GB/Z 24364-2009）

《信息安全管理体系要求》（GB/T 22080-2008）

《信息安全管理实用规则》（GB/T 22081-2008）

《信息系统安全管理要求》（GB/T 20269-2006）

《信息安全事件分类分级指南》（GB/Z 20986-2007）

《信息安全事件管理指南》（GB/Z 20985-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全应急响应计划规范》（GB/T 24363-2009）

（四）测评系统级别

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **等保测评级别** |
| 1 | HIS系统 | 三级 |
| 2 | LIS系统 | 三级 |
| 3 | PACS系统 | 三级 |
| 4 | 苏州科技城医院官网 | 二级 |

（五）相关承诺

响应单位须提供承诺：未因违规行为受到国家网络安全等级保护工作协调小组办公室或江苏省网络安全等级保护协调小组办公室的处罚。不提供承诺视为非实质性响应。

（六）项目工作内容

1.等级保护测评

根据等保2.0标准要求，对系统进行测评分析，对评估对象的现状作记录，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；按照用户系统现状对应的管理要求进行测评分析，对评估对象的现状作记录，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。

（1）识别信息安全风险。通过对信息系统在安全技术和安全管理方面的分析，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，并进行风险分析，出具差距分析报告，明确信息系统面临的风险。

（2）增强安全防护能力。依据差距分析报告的结果，并结合实际情况，区分轻重缓急，制定针对性的安全整改计划，通过安全整改不断提高信息系统的整体安全保护水平。

（3）测评结果分析

①单项测评结果判定

②单元测评结果判定

③整体测评分析

④形成测评分析报告

⑤针对测评分析报告的整改建议

2.渗透测试

选取可能发起攻击的测试点，使用渗透测试的方式查找可能存在的渗透点,发现信息系统防护体系的薄弱环节，找出可能发生的恶意攻击事件和违规行为。

（1）渗透测试的内容

* 工作内容包括渗透测试及提供漏洞修复方案。
* 本次渗透测试工作为黑盒测试。

（2）需要包含如下阶段

* 前期交互阶段：与用户组织进行讨论，确定渗透测试范围和目标。
* 信息搜集阶段：采用各种方法搜集用户方的所有相关信息。
* 威胁建模阶段：使用在信息搜集阶段所获取到的信息，标识出目标系统上可能存在的安全漏洞与弱点。
* 漏洞分析阶段：综合前面几个环节获取到的信息，从中分析和理解，找出攻击途径和攻击方法。
* 渗透攻击阶段：针对确定好的攻击途径和攻击方法实施渗透攻击，获取系统相关权限。
* 后渗透攻击阶段：以特定的业务系统作为目标，识别出关键的基础设施，找出用户组织最具价值和尝试进行安全保护的信息和资产，找出能够对用户组织造成重要业务影响的攻击途径。
* 报告阶段：将渗透测试结果编制成文档提交给用户，提供安全解决方案。并将在渗透测试阶段产生的垃圾数据进行清理。

（3）渗透测试工作要求

本次渗透攻击测试工作应当以不破坏用户应用系统为前提条件，不做危害用户应用系统的工作行为，遵守职业道德，遵守行业规则，严格遵守保密制度，保密要求，不得擅自修改、拷贝用户数据，不得泄露、传播用户的敏感信息，如有违反将负法律责任。

（七）服务成果

本次安全服务应提交以下成果：

1.《网络安全等级测评报告》，包括单元测评分析结果、整改测评分析结果、测评结论和安全整改建议等。

2.《信息系统渗透测试报告》，包含但不限于如下方面的内容：渗透测试的方法、目标、范围。测试的人员、时间、策略。测试的工具、风险规避措施。测试的过程、漏洞利用截图，测试的结果等。

3.提供培训服务，对业主单位信息安全管理相关人员进行安全意识教育，针对最新网络安全现状进行培训；指导信息安全管理制度的落实，并针对信息安全事故进行应急处置培训。

4. 提供安全技术支持服务，在项目工作期间，若业主单位发生网络安全问题，应及时提供远程或现场网络安全技术支持，帮助排查解决相关问题。

（八）服务人员要求

1.项目实施过程中，具有工作资质的项目组成员应不少于4人，其中项目经理1人。

2.项目实施过程中实行专人专职原则，保证各安全层面的测评全面有效，能够发现实际存在安全风险。

3.项目组人员必须熟练掌握信息安全相关标准与规范，具备丰富的信息安全测评工作经验，具有成熟的信息安全技术和项目管理能力，能够应对可能的突发性安全事件应急工作。

4.供应商应在项目开始前，应签订保密协议，严格遵守法律法规，对委托单位的商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经同意，严禁将上述内容与任何第三方透露或用于其他商业用途，并承担由此产生的一切损失。