## 采购需求

## 一. 项目概述

本项目共1个包，采购金堂县第一人民医院2021年网络安全等级保护测评服务

## 二.项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 包号 | 品目号 | 标的名称 | 所属行业 | 数量 |
| 01 | 01-01 | 安全等级保护测评服务 | 其他未列明行业 | 1项 |

## \*三.项目要求

**（一）、技术、服务要求**

**(1)测评内容包括技术和管理测评：**

1．技术安全性测评包括但不限于：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。

2．管理安全测评包括但不限于：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。

**(2)测评对象及范围**

本次等级保护测评系统包括：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 安全保护等级 |
| 1 | 医院网站 | 第三级 |
| 2 | HIS系统 | 第三级 |
| 3 | PACS系统 | 第三级 |
| 4 | LIS系统 | 第三级 |

**(3)依据标准**

①《中华人民共和国网络安全法》

②GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

③GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》

④GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》

⑤GB/T36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》

⑥《信息安全等级保护管理办法》公通字 [2007] 43号

⑦《网络安全等级保护测评机构管理办法》公信安 [2018] 765号

**(4)测评原则**

项目具体要求

对信息系统安全等级保护状况进行测试评估，应包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息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。

**（5）测评要求**

1）安全物理环境

| 序号 | 工作单元名称 | 工作单元描述 |
| --- | --- | --- |
| 1 | 物理位置选择 | 通过访谈、检查机房等信息系统物理场所在位置上是否具有防雷、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 通过访谈、检查主机房出入口、机房分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 通过访谈、检查机房的主要设备、介质和防盗报警系统等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 通过访谈、检查机房的设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 通过访谈、检查机房的设计/验收文档，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 通过访谈、检查机房的除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 通过访谈、检查机房是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 通过访谈、检查机房温、湿度情况，是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 通过访谈、检查机房供电线路、设备等过程，是否具备提供一定的电力供应的能力。 |
| 10 | 电磁防护 | 通过访谈、检查是否具备一定的电磁防护能力。 |

2）安全通信网络

| 序号 | 工作单元名称 | 工作单元描述 |
| --- | --- | --- |
| 1 | 网络架构 | 通过访谈、检查、测试网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络宽带分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性，以及通信线路、关键设备硬件冗余，系统可用性保证情况。 |
| 2 | 通信传输 | 通过访谈、检查、测试通信传输过程的数据完整性和保密性保护情况。 |
| 3 | 可信验证 | 通过访谈、检查通信设备的系统引导、系统程序、重要配置参数和通信应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。 |

3）安全区域边界

| 序号 | 工作单元名称 | 工作单元描述 |
| --- | --- | --- |
| 1 | 边界防护 | 通过访谈、检查、测试边界完整性检查设备，测评分析跨域边界的访问控制和数据流通过边界设备的控制措施，非法内联、外联、无线准入控制的监测、阻断等能力。 |
| 2 | 访问控制 | 通过访谈、检查、测试网络访问控制设备策略部署，测试系统对外暴露安全漏洞情况等过程，测评分析对进出网络的数据流量控制以及基于应用协议和应用内容的访问控制能力。 |
| 3 | 入侵防范 | 通过访谈、检查、测试网络边界处、关键网络节点检测、防止或限制从内部和外部发起网络攻击行为的防护能力，以及网络行为分析、监测、报警能力，特别是新型网络攻击行为的分析，对攻击行为的检测是否涉及攻击源、攻击类型、攻击目标、攻击事件、入侵报警等方面的防范能力。 |
| 4 | 恶意代码和防垃圾邮件 | 通过访谈、检查、测试关键网络节点处对恶意代码、垃圾邮件进行检测、防护和清除、恶意代码防护机制的升级和更新维护等情况， |
| 5 | 安全审计 | 通过访谈、检查网络边界、重要网络节点安全审计情况等，测评分析信息系统审计配置和审计记录保护，审计内容等情况。 |
| 6 | 可信验证 | 通过访谈、检查边界设备的系统引导、系统程序、重要配置参数和边界防护应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。 |

4）安全计算环境

| 序号 | 工作单元名称 | 工作单元描述 |
| --- | --- | --- |
| 1 | 身份鉴别 | 通过访谈、检查、测试对登录的用户进行身份标识和鉴别，是否具有不易被冒用的特点，口令应有复杂度要求并定期更换，以及远程管理安全、双因素鉴别等内容。 |
| 2 | 访问控制 | 通过访谈、检查、测试是否启用访问控制功能，依据安全策略控制用户对资源的访问；是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限等内容。 |
| 3 | 安全审计 | 通过访谈、检查安全审计范围及内容。 |
| 4 | 入侵防范 | 通过访谈、检查、测试是否能够检测到对重要节点进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警，是否遵循最小化安全装原则、系统服务、默认共享和高危端口、终端接入限制、数据有效性检验、已知漏洞防护等内容。 |
| 5 | 恶意代码防范 | 通过访谈、检查、测试是否具有防恶意代码攻击的技术措施或主动免疫可信验证机制，能否及时识别入侵和病毒行为并将其有效阻断等内容。 |
| 6 | 可信验证 | 通过访谈、通过访谈安全员，检查计算设备的系统引导、系统程序、重要配置参数和应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。 |
| 7 | 数据完整性 | 通过访谈、检查、测试重要数据在传输和存储过程中的完整性保护情况，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 |
| 8 | 数据保密性 | 通过访谈、检查、测试重要数据在传输和存储过程中的保密性保护情况，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 |
| 9 | 数据备份恢复 | 通过访谈、检查、测试重要数据本地备份与恢复功能，异地实时备份功能，以及重要数据处理系统的热冗余和高可用性保证等。 |
| 10 | 剩余信息保护 | 通过访谈、检查、测试边界信息在存储空间被释放或重新分配前是否有效清除，存有敏感数据的存储空间被释放或重新分配前是否有效清除等。 |
| 11 | 个人信息保护 | 通过访谈、检查、测试是否仅采集和保存业务必须的用户个人信息，对用户个人信息的访问和使用等。 |

5）安全管理中心

| 序号 | 工作单元名称 | 工作单元描述 |
| --- | --- | --- |
| 1 | 系统管理 | 通过访谈、检查、测试对系统管理员身份鉴别、命令或操作管理、操作审计，以及是否通过系统管理对系统资源和运行进行配置、控制和管理等。 |
| 2 | 审计管理 | 通过访谈、检查、测试对审计管理员身份鉴别、命令或操作管理、操作审计，以及是否通过审计管理员对审计策略、审计记录进行分析、处理等。 |
| 3 | 安全管理 | 通过访谈、检查、测试对安全管理员身份鉴别、命令或操作管理、操作审计，以及是否通过安全管理员对安全策略、参数进行配置等。 |
| 4 | 集中管控 | 通过访谈、检查、测试是否具有特定的管理区域，对分布在网络中的安全设备或安全组件进行集中管控，对网络链路、安全设备、网络设备和服务的运行进行集中监测，对分散在各设备上的审计数据进行收集汇总和集中分析，并确保记录留存符合法律法规要求，对安全策略、恶意代码、升级补丁等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析等。 |

6）安全管理制度

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 工作单元描述 |
| 1 | 安全策略 | 通过访谈、检查网络安全工作的总体方针我安全策略是否全面、完善。 |
| 2 | 管理制度 | 通过访谈、检查管理制度的制定和发布过程是否遵循一定的流程。 |
| 3 | 制度和发布 | 通过访谈、检查管理制度定期评审和修订情况。 |
| 4 | 评审和修订 | 通过访谈、检查管理制度在内容覆盖上是否全面、完善。 |

7）安全管理机构

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 工作单元描述 |
| 1 | 岗位设置 | 通过访谈、检查安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 通过访谈、检查各个岗位人员配备情况。 |
| 3 | 授权和审批 | 通过访谈、检查对关键活动的授权和审批情况。 |
| 4 | 沟通和合作 | 通过访谈、检查内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核和检查 | 通过访谈、检查安全工作的审核和检查情况。 |

8）安全管理人员

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 工作单元描述 |
| 1 | 人员录用 | 通过访谈、检查录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 通过访谈、检查人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 通过访谈、检查是否对人员进行安全方面的教育和培训。 |
| 4 | 外部人员访问管理 | 通过访谈、检查对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

9）安全建设管理

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 工作单元描述 |
| 1 | 定级和备案 | 通过访谈、检查是否按照一定要求确定系统的安全等级。 |
| 2 | 安全方案设计 | 通过访谈、检查整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 通过访谈、检查是否按照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 通过访谈、检查自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 通过访谈、检查外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 通过访谈、检查建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 通过访谈、检查系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 通过访谈、检查是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 通过访谈、检查等级测评、整改情况。 |
| 10 | 服务商选择 | 通过访谈、检查是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

10）安全运维管理

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 工作单元描述 |
| 1 | 环境管理 | 通过访谈、检查是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 通过访谈、检查是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 通过访谈、检查是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 通过访谈、检查是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 漏洞和风险管理 | 通过访谈、检查安全漏洞和隐患识别、处理情况，以及是否定期开展安全测评以及安全问题的应对措施。 |
| 6 | 网络和系统安全管理 | 通过访谈、检查是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。 |
| 7 | 恶意代码防范管理 | 通过访谈、检查是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 通过访谈、检查基本配置信息管理情况 |
| 9 | 密码管理 | 通过访谈、检查是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 通过访谈、检查是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 通过访谈、检查是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 安全事件处置 | 通过访谈、检查是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 通过访谈、检查是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
| 14 | 外包运维管理 | 通过访谈、检查外包运维服务商选择是否符合国家要求，外包运维保密、服务内容管理等。 |

11）安全扩展要求

按照所测评系统的具体情况选用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、工业控制系统安全扩展要求。

12）验证测试相关要求

按照等级保护测评要求，测评过程中应配备必要的工具、仪器/设备对信息系统进行验证测试，采用的测评工具的生产商应为正规厂商， 能够对产品进行持续更新并提供质量和安全保障。

验证测试内容包括但不限于以下内：

1.渗透测试

验证安全策略正确性；保证用户登录窗体身份验证的安全性；非授权用户不能浏览到未授权内容；不存在跨站点脚本攻击漏洞；脚本不存在SQL、Cookie注入漏洞；安全的处理异常，没有出错页面泄露系统信息；应用和系统漏洞及其他，并提出整改建议。验证内容包括（但不限于）以下几个方面：

|  |  |
| --- | --- |
| 注入 | 失效的身份认证 |
| 敏感信息泄露 | XML外部实体（XXE） |
| 失效的访问控制 | 安全配置错误 |
| 跨站脚本（XSS） | 不安全的反序列化 |
| 使用含有已知漏洞的组件 | 不足的日志记录和监控 |

2．性能测试

通过模拟手段对网络（包括丢包、时延、带宽等）、软件系统（包括负载、响应）、负载下硬件占用（包含CPU、内存）等进行全面的测评评估验证系统的可靠性、可用性，通过对测试结果的分析，给出相应的整改建议。

3．漏洞扫描

据相关标准、规范要求对重要信息系统的安全漏洞进行测评。分析总结系统中存在的主要安全漏洞，指出系统中可能被利用的安全漏洞、系统配置错误等缺陷以及相应的安全加固意见、建议。

**（二）.测评工作步骤**

受委托测评机构对信息系统的初次等级测评可以分为四项活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。供应商应对等级保护测评各阶段具体工作内容进行描述。

1.准备活动阶段：对被测系统进行调研分析，明确测评对象、测评方法等工作。

2.方案编制阶段：制定信息安全等级保护测评项目计划书、测评实施方案，并提交委托方确认。

3.现场测评阶段：按照等级保护相关标准规范要求从访谈、检查、测试几方面进行测试评估并出具《整改意见》，并在整改过程中提供技术咨询服务。

4.分析与报告编制：向委托方提交被测信息系统安全等级保护测评报告以及相应文档。

**（三）.实施要求**

1．系统梳理

协助金堂县第一人民医院完成待测信息系统梳理工作。

2．初测

对本项目所涉及信息系统进行现场测评，初次测评完成后提交初评的整改意见报告。

3．整改加固协助

协助金堂县第一人民医院对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。

4．成果递交

整理测评结果，提交被测信息系统安全等级保护测评报告以及相应文档。

**（四）.项目管理与实施保障**

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，供应商必须提供完整的项目管理方案，并符合以下要求：

1．供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任。

2．应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力。

3．供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留。

4．供应商的岗位配置要至少配置测评工程师、总测评工程师、技术主管、质量主管、保密安全员和档案管理员，其中项目经理、技术主管、质量主管、保密安全员和档案管理员应独立配置，不能有兼任的情况。

5．测评人员要求

参与此次等级保护测评的供应商其测评人员应具备并符合以下要求：

（1）开展此次等级保护测评工作的人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

（2）开展此次等级保护测评工作的人员应由取得等级测评师证书（等级测评人员应由初级、中级和高级）的人员组成。

（3）开展此次等级保护测评工作的人员应具备从事信息系统安全测评相关工作三年以上工作经验，开展等级保护测评工作不少于一年，参与同类行业信息安全测评项目。

（4）针对软件、网络、安全等方面的测评技术人员除具有信息安全等级保护测评师证书以外，还应该持有相关技术资格证书。

（5）测评项目组人员在对开展等级保护测评工作之前需签订保密协议。

6．测评工具要求

（1）采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件。

（2）采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品。

（3）测评机构所使用的测评工具不会对系统产生破坏或负面影响。

**\*四、商务要求**

1．服务期限及地点

1.1 服务期限：合同签订后45工作日完成所有工作，因采购人原因工期延期的供应商可以书面形式申请工期顺延。

1.2 服务地点：采购人指定地点。

2．付款方法和条件：合同签订后供应商向采购人开具正式发票（含税）等付款凭证资料递交给采购人，采购人在收到成交供应商相关资料后按季度支付。

3、提供一年维保服务，维保内容：提供信息网络安全咨询服务；每季度对采购人信息网络安全进行测试分析并给出报告。