**温州医科大学附属眼视光医院**

**服务需求审批表**

|  |  |
| --- | --- |
| 项目名称 | 等级保护测评服务 |
| 预算号： | / | 预算金额： | 16万元 |
| 服务要求 |
| 序号 | 摘要 | 内容 |
| 1 | 依据标准 | 投标供应商应依据国家等级保护相关标准开展工作，依据标准（包括但不限于）如下国家标准：GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求；GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求。 |
| 2 | 测评内容 | 根据国家等级保护相关标准，投标供应商两年内完成4个三级系统，1个二级系统等级保护测评工作。信息系统安全等级保护测评的内容（包括但不限于）以下内容：根据用户单位信息系统的保护等级，并依据GB/T 22239-2019 信息安全技术网络安全等级保护基本要求的条款要求，全面分析应用系统的安全保护措施与等级保护相应级别之间的差距，进行合规性分析，为系统等级保护加固整改提供客观依据，配合委托方督促集成商根据安全改进建议进行适度加固整改，测评的内容包括但不限于以下内容：安全通用要求（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）及扩展项要求。项目验收完成后，要求提供为期一年的安全咨询服务，7\*24响应支持。 |
| 3 | 技术服务 | 测评应满足的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：a、保密原则：对测评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，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究投标供应商的责任。b、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。c、规范性原则：投标供应商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。d、可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。e、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。f、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。安全测评报告a、投标供应商应协助采购人对其信息系统进行定级与上报到温州市网信办进行专家评审。b、投标供应商应对采购人的信息系统进行等级保护测评，形成相应的报告。c、投标供应商在测评后出具符合公安局要求的系统安全保护等级测评报告；d、对上述系统不符合信息安全等级保护有关管理规范和技术标准的，投标供应商应协助采购人进行整改并出具可行整改方案。e、投标供应商协助采购人办理信息系统安全保护等级测评备案手续，直至采购人拿到公安相关部门出据的备案证明。 |
| 4 | 本次等级保护测评的整体要求 | A、投标供应商应提供定级咨询服务，辅助编制定级报告、定级备案表。B、投标供应商应提供等级保护测评政策宣贯及前期工作培训。C、投标供应商应提供现场测评完成后的整改建议服务；D、投标供应商应详细描述本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、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。E、投标供应商应安排高级测评师带队到现场，进行本次等级保护测评工作。投标供应商应详细描述测评人员的组成、资质及各自职责的划分。F、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投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。在报价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。G、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。H、安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。I、安全测评需要的运行环境（如场地、网络环境等）由采购人提供，投标供应商应详细描述需要的运行环境的具体要求。J、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。 |
| 5 | 项目实施要求 | A、投标供应商应保证投标项目在采购方条件成熟时应立即开展实施；B、投标供应商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，投标供应商必须执行，在采购方限定的时间内解决问题。如果投标供应商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；C、投标供应商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；D、投标供应商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；E、本次项目实施人员至少包含1名高级测评师，同时具备国家注册信息安全专业人员（CISP）证书、信息安全保障人员认证证书(CISAW) 、注册网络安全渗透评估专业人员（NSATP-A）证书。本次实施扫描、渗透服务工程师需具备注册渗透测试工程师(CISP-PTE)证书。F、三年内未被国家网络安全等级保护工作协调小组办公室责令整改的测评机构G、项目验收完成后，要求提供为期两年的安全咨询服务，以保证项目正常运行。 |
| 6 | 项目验收 | 本次项目验收以通过公安及相关部门的备案为准，即每个系统都拿到相应的备案证明视为验收合格。 |
| 7 | 项目承诺 | 投标供应商应满足采购人提出的标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质。保密性要求：投标供应商必须和采购人签订保密协议和非侵害性协议，投标供应商必须要与参加此次测评项目的所有项目组成员签订保密协议和非侵害性协议，在合同签定时一并提供给采购人。投标供应商具体测评工作和等级保护测评报告的编写，必须在采购人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，投标供应商不得带离该地点。投标供应商对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标供应商中标与否，其对上述内容的保密责任将长期存在。等级保护测评的品质保证：投标供应商应承诺指派工作经验丰富、技术实力雄厚的安全顾问，结合技术领先、结论可靠的测评工具为客户作全面等级保护测评。承诺测评过程按照国家标准进行，并保证对客户的资料严格保密。 |
|  | 其它要求 | 投标供应商在测评方案书中，对能提供的信息系统安全等级保护测评进行详细说明，可根据具体情况在项目方案中提出建议，并附详细资料和说明。投标供应商应对提供测评服务时所使用的设备及软件保证拥有设备软硬件的知识产权和所有权，并对所涉及的专利、知识产权等法律条款承担义务，采购人以上问题不承担任何法律责任。若投标供应商的设备和系统包含自己的专用标准，应在建议书中具体说明，并附上相应的详细技术资料。投标供应商提供测评服务期间，接到采购人服务请求后3天内到达指定场所配合测评工作。针对本单位的系统提供一年不少于4次的扫描、渗透服务，并对扫描结果予以验证。投标供应商在进行测评的时候必须进行渗透测试，并提交渗透测试报告 |
|  | 项目成果 | 提交包括且不仅仅包括以下成果：《信息系统安全等级保护测评实施方案》（按需）《信息系统安全整改规划》《信息系统等级保护测评报告》《信息系统安全等级保护备案表》与定级报告（按需） |
|  | 商务要求 | 合同期限 | 本合同有效期为合同签订后，接到甲方通知启动该项目之日起信息系统等级保护测评服务两年或本合同总金额履行完毕时止，以先到为准。 |
| 第一阶段：签订合同后，乙方应在2025年12月前完成当年等级保护系统测评。第二阶段：乙方应于2026年12月前完成当年等级保护测评。 |
| 付款方式 | 完成第一阶段等保测评并提交等级保护测评报告通过备案，待乙方提供正规发票后，甲方向乙方支付50%货款；完成第二阶段等保测评并提交等级保护测评报告通过备案，待乙方提供正规发票后，甲方向乙方支付50%货款。 |
| 甲乙双方应当严格履行合同，确保本项目如期完成，如在本项目实施过程中，因甲方原因导致项目无法推进，乙方应当立即出具《告知函》给甲方，要求其排除障碍，并经甲方确认（需双方盖章），从该问题产生到消除，其所消耗的时间可不计入项目工期，若乙方未告知甲方排除障碍，视为符合乙方实施项目建设要求。 |
| 申请科室 | 信息管理部 | 需求部门经手人 |  |
| 采购部门经手人 |  | 需求部门负责人 |  |
| 采购部门负责人 |  | 信息管理部负责人 | / |
| 需求部门分管领导 | / | 申请时间 |  |