采购招标项目参数要求表格说明

一、本表格为细化预算参数使用，所填参数不可与已获批申购预算有冲突，如有冲突以学校已批文件为准。

二、技术指标里不得含有排他性技术指标（申购预算里已指定品牌型号的除外），如经核实指标单条或多条组合具有排他性的，根据相关规定，需经使用单位修改或补充书面说明后方可启动招标或谈判程序。根据需要指定品牌时，亦需附相关说明。

三、本参数一经挂网公示，原则上不允许修改，如确有需要修改的，按照学校《吉林大学珠海学院采购与招标管理办法》第二十九条之规定，在招标公告发布3天内向采购中心提交暂停采购的书面报告。

四、招标会议开始后，原则上不允许现场增减参数要求，如发现有重要参数指标缺失将对学校造成重大利益损失的，招标会议立即终止，现场宣布流标，会后使用单位需以书面形式向采购招标领导小组说明情况。

采购招标项目参数要求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | | 吉林大学珠海学院网络安全服务 | | 采购编号 | | CG2018 |
| 供货时间 | | 2019.9.25 | | 供货地点 | | 吉林大学珠海学院 |
| 售后服务要求 | | 1年期 | | 安装调试要求 | | 如期提供服务 |
| 项目概述：  网络安全服务主要包含以下内容：   1. 风险评估服务 ：依据相关规范，在用户允许的情况下，对目标范围内的系统资产、威胁、脆弱性等各方面进行评估，对主要资产的风险进行定性或定量的脆弱性风险分析，描述不同资产的风险高低状况，给出详细的风险评估报告、整改方案及技术支撑。 **每月一次并出具风险评估报告。** 2. 威胁监测与主动响应服务：外聘安全专家对现有安全设备、态势感知的安全日志、流量进行关联分析，主动识别网络和主机中的安全威胁，协助客户处置安全事件，并提供加固建议。 **每周一次。** 3. 漏洞扫描服务：依据相关规范，通过现场方式使用专业的国产漏洞扫描工具对信息系统进行全面漏洞扫描工作，为安全加固提供安全建议。 **每月一次并出具漏洞扫描结果报告。**   ①漏洞扫描应按照以下要求实施：  漏洞扫描服务流程：   * 服务商应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 * 服务商应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描申请，在用户授权后，方可进行。 * 服务商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性。   服务商应提交针对性的解决方案，保证漏洞修复可落地。  漏洞扫描工具支持对象应包含但不限于：   * 网络设备：路由器、交换机、防火墙等； * 操作系统：windows、linux、UNIX等； * 数据库：Oracle、MS SQL、Mysql等；   中间件：Apache、Tomcat、weblogic等。  漏洞扫描参数应包含但不限于：版本漏洞、开放端口、开放服务、空/弱口令账户、安全配置等。  服务商提供的漏洞扫描工具应具备对高可利用漏洞的管理（需提供截图证明并加盖原厂商公章）。  服务商提供的漏洞扫描工具应具备对扫描出或已修复的漏洞，具备一键复测功能（需提供截图证明并加盖原厂商公章）。   1. 应急演练服务：协助单位制定应急响应机制，完善应急响应预案，并根据用户实际情况，提供应急事件演练方案。 每月一次。 2. 应急响应服务：针对单位突发的安全事件，提供问题应急处置，恶意文件清除并协助恢复业务，针对问题进行入侵原因分析，找到攻击路径。 **全年为单位，不低于平均每月二次。** 3. 信息安全培训：   ①安全意识培训：提供包括信息安全的重要性，相关信息安全事件案例分析及操作运维人员职责范围内需要注意的安全问题。**每月开展一次。**  ②安全技术培训：提供主流的黑客攻防技术和工具的使用以及攻击行为的特征等，帮助运维人员了解攻击原理，掌握应对方法。**每月开展一次。**  7.渗透测试：对应用系统模拟黑客攻击进行安全性测试，发现系统存在的安全问题，对过程中发现的问题及风险提出安全加固建议。**每月开展一次。**  8.人员驻场：安全厂商专业安服人员（具备PMP、CISSP、CIIP-A、CCSSP、CISP、ISO27001和CISAW应急服务专业级证书）驻场值守一年，全方位保障单位安全。 | | | | | | |
| **重要技术指标（必填）** | | | | | | |
| 序号 | 指标名称 | 参数明细 | | | | |
| 1 | 实施方案 | 根据招标文件的要求，应从技术团队、技术方案、项目管理等方面确保其完整性、合理性、先进性等。 | | | | |
| 2 | 项目重点难点分析、应对措施及相关的合理化建议 | 根据招标文件的要求，对学校网络、信息化整体状况有充分的了解和分析，对本项目的服务内容进行重点难点分析，对提供合理有效的解决办法。 | | | | |
| 3 | 质量（完成时间、安全、管理）保障措施及方案 | 根据本项目服务要求，结合学校当前情况和整个国际、国家网络安全状况，有针对性的提出质量保障实施方案，具体包括信息安全服务质量保障流程、进度计划等进行横向比较。 | | | | |
| 4 | ★拟安排的项目经理情况 | 为保障项目服务质量和实施进度，服务商的项目经理需具备以下证书：PMP、CISSP、CIIP-A、CCSSP、CISP、ISO27001和CISAW应急服务专业级证书,要求提供通过服务商购买的项目负责人近半年的社保证明、相关证书，以上资料均要求提供扫描件加盖公章。 | | | | |
| 5 | ★拟安排的服务商工程师（主要技术人员）情况 | 1、拟安排实施的服务人员，至少拥有CISAW（应急服务）证书、CISAW（风险管理）证书、CISSP证书的。要求提供通过服务商购买的项目主要团队成员（主要技术人员）的近半年的社保证明和相关证书作为得分依据。以上资料均要求提供扫描件加盖公章。 | | | | |
| 6 | ★服务商技术实力 | CCRC信息安全服务资质认证证书—信息安全风险评估服务一级资质、服务商具备CCRC信息安全服务资质认证证书—信息安全应急处理服务一级资质、信息安全等级保护建设服务机构能力评估合格证书、CMMI 5认证证书、国家信息安全测评服务资质证书—安全工程类一级。以上证书投标服务商应具备3个及以上。  以上资料均要求提供扫描件。  要求服务商在珠海市设立办公场所。要求有官网可查的省内办事机构。 | | | | |
| **一般技术指标（选填，不作为评标依据）** | | | | | | |
| 序号 | 指标名称 | 参数明细 | | | | |
| 1 |  |  | | | | |
| 2 |  |  | | | | |
| 3 |  |  | | | | |
| 4 |  |  | | | | |
| 申报人 | |  | | | 单位负责人 |  |
| 实验室与资产管理处 | | |  | | | |

**注： 1、参数不可与已获批学年采购预算有冲突，如有冲突以已批准采购文件为准2、不得含有排他性技术指标3、条目可根据具体情况增减4、本页不够可另起一页。**