成都汽车职业技术学校

网络二级等保测评项目

比

选

文

件

成都汽车职业技术学校 编制

2025年04月

# 比选公告

# 成都汽车职业技术学校网络二级等保测评项目公告

成都汽车职业技术学校拟对成都汽车职业技术学校网络二级等保评测项目进行比选。兹邀请符合本次比选条件的比选申请人参加。

**一、项目名称：成都汽车职业技术学校网络二级等保评测项目**

**二、项目编号：QCZX-QC-20250427**

**三、比选申请人参加本次比选活动应具备下列条件：**

1、具有独立承担民事责任的能力；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、具有依法缴纳税收和社会保障资金的良好记录；

5、参加本次采购活动前三年内，在经营活动中没有重大违法记录；

6、法律、行政法规规定的其他条件；

7、根据采购项目提出的特殊条件。（详见比选文件第四章）

**三、比选文件发售方式：**

比选文件详见公告下方附件1。

1. **比选申请文件提交方式及截止时间：**

比选申请文件格式要求：**盖章密封纸质版文件**

递交地址：**成都汽车职业技术学校总务处（成都市龙泉驿区同安镇幸福路388号）**

递交截止时间：**2025年04月30日12时00分（北京时间），**逾期递交的比选文件恕不接收。

提交比选申请文件时必须同时提交以下资料：

（1）单位介绍信；

（2）经办人身份证复印件及联系方式。（法定代表人投标需提供法定代表人身份证复印件及营业执照复印件），以上材料均须加盖公章。

**五、比选时间：2025年4月30日14时00分（北京时间）**。

**六、比选地点：**成都汽车职业技术学校（成都市龙泉驿区同安镇幸福路388号）。

**七、本比选邀请在成都汽车职业技术学校官网上以公告形式发布，本项目不属于政府采购项目。**

**八、联系方式**

**采购人：**成都汽车职业技术学校

地址：成都市龙泉驿区同安镇幸福路388号

联 系 人：高老师

联系电话：028-68389129,13228133989

# 投标人须知

项目名称：成都汽车职业技术学校网络二级等保评测项目

编号：QCZX-QC-20250427

最高限价：49000.00元

具体服务内容包括：

（1）测评对象：成都汽车职业技术学校，合同周期内完成一次等级保护测评。

（2）协助业主单位进行信息系统的信息安全等级为二级的备案工作。

（3）等保测评：

至少包括以下内容：

安全技术测评。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、安全管理中心方面的安全测评。

安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果编制测评报告，制定并提交《网络安全等级测评报告》。

（4）协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

（5）测评指标

| **分类** | **子类** | **基本要求** |
| --- | --- | --- |
| 安全物理环境 | 物理位置选择 | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内;b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
| 物理访问控制 | 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。 |
| 防盗窃和防破坏 | a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识;b) 应将通信线缆铺设在隐蔽安全处。 |
| 防雷击 | 应将各类机柜、设施和设备等通过接地系统安全接地。 |
| 防火 | a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火;b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。 |
| 防水和防潮 | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透;b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。 |
| 防静电 | 应采用防静电地板或地面并采用必要的接地防静电措施。 |
| 温湿度控制 | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |
| 电力供应 | a) 应在机房供电线路上配置稳压器和过电压防护设备;b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。 |
| 电磁防护 | 电源线和通信线缆应隔离铺设，避免互相干扰。 |
| 安全通信网络 | 网络架构 | a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址;b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。 |
| 通信传输 | 应采用校验技术保证通信过程中数据的完整性。 |
| 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信 验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全区域边界 | 边界防护 | 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。 |
| 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信;b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化;c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出;d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。 |
| 入侵防范 | 应在关键网络节点处监视网络攻击行为。 |
| 恶意代码防范 | 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。 |
| 安全审计 | a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| 可信验证 | 可基于可信根对边界设备的系统引导程序、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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全计算环境 | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| 访问控制 | a) 应对登录的用户分配账户和权限;b) 应重命名或删除默认账户，修改默认账户的默认口令;c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在; d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| 安全审计 | a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| 入侵防范 | a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;b) 应关闭不需要的系统服务、默认共享和高危端口;c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| 恶意代码防范 | 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。 |
| 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 数据完整性 | 应采用校验技术保证重要数据在传输过程中的完整性。 |
| 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能;b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| 剩余信息保护 | 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 |
| 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息; b) 应禁止未授权访问和非法使用用户个人信息。 |
| 安全管理中心 | 系统管理 | a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对 这些操作进行审计; b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、 系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
| 审计管理 | a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计;b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| 安全管理制度 | 安全策略 | 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全 框架等。 |
| 管理制度 | a) 应对安全管理活动中的主要管理内容建立安全管理制度;b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。 |
| 制定和发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定;b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |
| 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制 度进行修订。 |
| 安全管理机构 | 岗位设置 | a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责;b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 |
| 人员配备 | 应配备一定数量的系统管理员、审计管理员和安全管理员等。 |
| 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等; b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。 |
| 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题;b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通;c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
| 审核和检查 | 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |
| 安全管理人员 | 人员录用 | a) 应指定或授权专门的部门或人员负责人员录用;b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。 |
| 人员离岗 | 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设 备。 |
| 安全意识教育和培训 | 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 |
| 外部人员访问管理 | a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案; b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案;c) 外部人员离场后应及时清除其所有的访问权限。 |
| 安全建设管理 | 定级和备案 | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由;b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定; c) 应保证定级结果经过相关部门的批准;d) 应将备案材料报主管部门和相应公安机关备案。 |
| 安全方案设计 | a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施;b) 应根据保护对象的安全保护等级进行安全方案设计;c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
| 产品采购和使用 | a) 应确保网络安全产品采购和使用符合国家的有关规定;b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。 |
| 自行软件开发 | a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制;b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。 |
| 外包软件开发 | a) 应在软件交付前检测其中可能存在的恶意代码; b) 应保证开发单位提供软件设计文档和使用指南。 |
| 工程实施 | a) 应指定或授权专门的部门或人员负责工程实施过程的管理;b) 应制定安全工程实施方案控制工程实施过程。 |
| 测试验收 | a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告; b) 应进行上线前的安全性测试，并出具安全测试报告。 |
| 系统交付 | a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点; b) 应对负责运行维护的技术人员进行相应的技能培训;c) 应提供建设过程文档和运行维护文档。 |
| 等级测评 | a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改;b) 应在发生重大变更或级别发生变化时进行等级测评;c) 应确保测评机构的选择符合国家有关规定。 |
| 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定;b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。 |
| 安全运维管理 | 环境管理 | a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等;c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
| 资产管理 | 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 |
| 介质管理 | a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点;b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |
| 设备维护管理 | a) 应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。 |
| 漏洞和风险管理 | 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响 后进行修补。 |
| 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限;b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制;c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定;d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等;e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。 |
| 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等;b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等;c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。 |
| 配置管理 | 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和 补丁信息、各个设备或软件组件的配置参数等。 |
| 密码管理 | a) 应遵循密码相关国家标准和行业标准;b) 应使用国家密码管理主管部门认证核准的密码技术和产品。 |
| 变更管理 | 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。 |
| 备份与恢复管理 | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等;b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等;c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 |
| 安全事件处置 | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等;c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。 |
| 应急预案管理 | a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容; b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。 |
| 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定;b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。 |

验收标准：

网络安全等级保护二级评测验收标准主要依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）和《信息安全技术 网络安全等级保护测评要求》（GB/T 28448）等国家标准。以下是二级等级保护评测验收的主要标准和要求：

验收内容

1、安全物理环境

物理位置选择：核查建筑物抗震设防审批文档、机房防水防雨及建筑结构状况。

物理访问控制：检查机房出入口门禁系统及值守记录、重要区域第二道门禁系统。

防盗窃和防破坏：查看设备固定及标识、通信线缆铺设、防盗报警或视频监控系统。

防雷击：检查机房设备接地处理、防感应雷措施及防雷装置检测情况。

防火：检查火灾自动消防系统、建筑材料耐火等级及区域防火隔离措施。

防水和防潮：查看机房防水、防潮措施及漏水检测报警装置。

防静电：检查防静电地板、接地措施及防静电设备配备。

温湿度控制：核查温湿度调节设施及温湿度范围。

电力供应：检查稳压器、过电压防护设备、备用电源、冗余电缆线路及应急供电设施。

电磁防护：查看电源线和通信线缆铺设、关键设备或区域电磁屏蔽。

2、安全通信网络

网络架构：检查网络设备性能、带宽、区域划分与地址分配、网络区域部署及冗余情况。

通信传输：核查数据完整性、保密性保护技术措施及通信双方验证认证情况。

可信验证：检查基于可信根的验证、动态验证、报警及审计记录等情况。

3、安全区域边界

边界防护：检查边界设备访问控制、非法设备接入检测与阻断、无线网络使用限制。

访问控制：查看访问控制策略设置、规则优化、基于多种条件的访问控制及协议转换或隔离。

入侵防范：核查网络攻击检测、防范及分析能力，以及攻击记录与报警。

恶意代码和垃圾邮件防范：检查关键节点防范措施及机制升级更新。

安全审计：检查审计系统部署、审计范围、记录内容及保护备份。

可信验证：查看基于可信根的验证、动态验证、报警及审计记录关联感知。

4、安全计算环境

身份鉴别：检查用户身份鉴别措施、登录失败处理、远程管理安全及多种鉴别技术使用。

访问控制：查看账户权限管理、默认账户处理、权限分离及访问控制粒度。

安全审计：核查审计功能启用、记录内容、保护备份及进程保护。

入侵防范：检查组件安装、系统服务关闭、端口限制、漏洞检测与修复。

恶意代码防范：检查主动免疫可信验证机制及入侵阻断。

可信验证：查看基于可信根的验证、动态验证、报警及审计记录关联感知。

数据完整性：核查数据传输、存储完整性保护及抗抵赖措施。

数据保密性：检查数据传输、存储保密性保护。

数据备份恢复：检查本地及异地备份功能、备份策略及系统热冗余。

5、安全管理中心

系统管理：检查系统管理员身份鉴别、操作审计及系统资源管理。

审计管理：核查审计管理员身份鉴别、审计操作审计及记录分析处理。

安全管理：查看安全管理员身份鉴别、安全策略配置及操作审计。

集中管控：检查安全设备管控、信息传输路径安全、运行状况监测及审计数据管理。

6、安全管理制度

安全策略：核查总体方针策略文档内容。

管理制度：查看各类安全管理制度覆盖范围及操作规程。

制定和发布：检查制度制定部门、发布方式及版本控制。

评审和修订：检查制度评审修订记录。

7、安全管理机构

岗位设置：核查机构设置、岗位划分及职责定义。

人员配备：检查人员配备情况。

授权和审批：查看授权审批事项、流程及审查更新。

沟通和合作：检查内部外部沟通合作机制及记录。

审核和检查：核查安全检查执行及报告情况。

8、安全管理人员

人员录用：检查录用流程、人员审查及协议签署。

人员离岗：检查离岗人员权限终止及手续办理。

安全意识教育和培训：核查培训计划、内容及考核记录。

外部人员访问管理：查看外部人员访问审批、陪同、登记及权限管理。

9、安全建设管理

定级和备案：核查定级文档、论证审批及备案情况。

安全方案设计：查看安全措施选择、整体规划设计及论证审批。

产品采购和使用：检查产品采购合规性、选型测试及密码产品管理。

自行软件开发：检查开发环境、制度、代码规范及安全测试。

外包软件开发：核查软件交付检测、文档提供及源代码审查。

工程实施：检查工程管理部门、实施方案及监理情况。

测试验收：查看测试验收方案、报告及上线前安全测试。

系统交付：检查交付清单、技术培训及文档提供。

等级测评：核查测评周期、机构选择及整改情况。

服务供应商管理：检查供应商选择、协议签订及服务监督。

10、安全运维管理

环境管理：检查机房安全管理、出入登记及设施维护记录。

资产管理：核查资产清单、标识管理及信息分类。

介质管理：查看介质存放、使用及传输管理。

设备维护管理：检查设备维护制度、审批及报废处理。

漏洞和风险管理：检查漏洞识别、修复及安全测评报告。

网络和系统安全管理：核查管理员角色划分、账户管理、制度制定及操作记录。

恶意代码防范管理：检查防恶意代码意识提升及措施有效性验证。

配置管理：查看配置信息记录、变更管理及信息库更新。

密码管理：检查密码使用合规性及产品认证。

变更管理：核查变更方案、申报审批及恢复程序。

备份与恢复管理：检查备份策略、计划及恢复测试。

安全事件处置：检查事件报告、处置制度及记录分析。

应急预案管理：核查预案框架、制定、培训演练及修订。

外包运维管理：检查外包商选择、协议签订及能力要求。

说明：

1. 所采购产品为含税开票价格，并为一次性报价。
2. 询价表格式：**盖章密封纸质版文件**。
3. 所供测评服务应达到等级保护测评相关标准。
4. 本项目不收取比选保证金。
5. 招标方式：询价招标（技术方案符合性审查通过后，以最低报价者中标）
6. 付款方式：二级等保测评完成，验收合格后，支付总金额的100%。

# 投标文件格式

一、本章所制投标文件格式，除格式中明确将该格式作为实质性要求的，一律不具有强制性，但投标人提交的投标文件可能影响评审小组评判的，可能作无效处理。

二、本章所制投标文件格式有关表格中的备注栏，由投标人根据自身情况作解释性说明，不作为必填项。

**成都汽车职业技术学校网络二级等保评测项目**

**投**

**标**

**报**

**价**

**文**

**件**

投标人： （盖章）

日 期：

一、法定代表人授权书

成都汽车职业技术学校：

 本授权声明： 法定代表人授权我方为我方代理人。代理人根据授权，以我方名义参成都汽车职业技术学校成都汽车职业技术学校网络二级等保评测项目投标报价事宜。

法定代表人 (签字或盖章) ：

授权代表(签字或盖章)：

投标人名称： （盖章）

日 期：

附件一：报价函密封袋封面样式

(填写采购项目名称、编号)

报 价 单

投标单位名称 ：

地址 ：

联系电话 ：

报价日期 ：

附件二：报价函样式

报价函

采购项目编号:

**致：XXX**

我公司已认真阅读了贵方发布的（项目编号）采购公示，接受贵方提出的各项要求，参与该项目报价。

1. 报价表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 品名 | 型号 | 单位 | 数量 | 单价（元） | 金额（元） |
| 1 | **成都汽车职业技术学校网络二级等保测评** | 二级 | 个 | 1 |  |  |
| **总价（元）****备注：以上价格含增值税普通发票** |  |

二、技术支持与服务承诺

三、有关资质证明材料

四、联系方式

联 系 人： 固定电话：

手机号码：

地　　址：

 供应商名称（盖章）：

 法人代表（印章）：

 　　　　　　　　　年  月  日

1. 公司相关资料（必须含营业执照）
2. 类似业绩

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目业主 | 项目名称 | 建设规模 | 合同价格（元） |
|   |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

五、承诺函

成都汽车职业技术学校：

我公司作为本次比选项目的投标人，根据比选文件要求，现郑重承诺如下：

一、我公司具备以下要求：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件；

二、我公司不属于禁止参加本次采购活动的投标人：

1、不属于列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的单位。

2、法律、行政法规规定的其他情形。

三、信誉要求：

我公司未处于财产被接管、冻结、破产状态，未处于四川省行政区域内有关行政处罚期间。单位及其现任法定代表人、主要负责人在前三年内不得具有行贿犯罪记录。

本公司对上述承诺的内容事项真实性负责。

投标人： （单位盖章）。

法定代表人/单位负责人或授权代表（签字）： 。

日期: 。

# 资格审查

资格审查由成都汽车职业技术学校组建资格审查小组依据法律法规和比选文件的规定，对投标人投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格。

资格审查标准见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 审查项目 | 合格条件 | 结论 |
| 1 | 在中华人民共和国境内依法成立的法人或其依法设立的分支机构 | 1. 投标人是法人的：要求提供有效期内的企业法人营业执照复印件（正本或副本），并加盖公章。
2. 投标人是其他组织的，要求提供营业执照复印件（正本或副本），并加盖公章。
 |  |
| 2 | 信誉要求 | 未处于财产被接管、冻结、破产状态，未处于四川省行政区域内有关行政处罚期间。单位及其现任法定代表人、主要负责人在前三年内不得具有行贿犯罪记录。要求投标人提供承诺书。 |  |
| 3 | 企业法人（或主要负责人）授权书/法定代表人身份证 | 按比选文件第三章“投标文件格式”的要求和格式填写 |  |
| 4 | 投标文件组成 | 符合比选文件第三章第四节第八条比选文件的构成“投标文件的组成”规定要求。 |  |
| 5 | 投标文件签字、盖章 | 均按比选文件第三章要求签字、盖章。 |  |
| 6 | 特殊项目要求 | 供应商具有《网络安全服务认证证书等级保护测评服务认证》证书 |  |

注：（1）上述全部符合合格条件的其结论为通过，通过资格审查的投标人才能进入本库，其中任何一项不符合合格条件的其结论为不通过，未通过资格审查的投标人本次不能入库，其投标文件按无效投标文件处理。如果评审小组认为投标人有任意一项不通过的，应在资格性审查报告中载明不通过的具体原因。

（2）在本次比选活动中，递交投标文件或通过资格审查投标人不足3家的，本次比选活动失败，另行组织新的比选活。