**2022年官网三级测评服务**

采购编号：TZY-ZB-2022012

**招**

**标**

**文**

**件**

采 购 人: 四川铁道职业学院

四川·成都

2022年06月

## 目 录

[第一章 投标邀请 1](#_Toc358883241)

[第二章 投标人须知](#_Toc358883242) 3

[第三章 投标文件格式](#_Toc358883243) 9

[第四章 招标项目技术、商务及其他要求 1](#_Toc358883246)8

[第五章 评标办法](#_Toc358883247)31

[第六章 合同主要条款](#_Toc358883248) 35

# 第一章 投标邀请

四川铁道职业学院就2022年官网三级测评服务项目进行公开招标，兹邀请符合本次招标要求的供应商参加投标。

**一、招标编号：**

**二、招标项目：2022年官网三级测评服务**

**三、资金来源：**财政资金

**四、招标项目简介：**

详见第四章

**五、供应商参加本次政府采购活动应具备下列条件：**

投标人必须符合《政府采购法》第二十二条要求，且满足以下条件：

1、投标人应为在中华人民共和国境内注册取得营业执照和税务登记证的独立法人；具有良好的商业信誉和健全的财务会计制度；具有履行合同所必需的设备和专业技术能力；有依法缴纳税收和社会保障资金的良好记录；企业法人营业执照已通过本年度年审；且所投产品在其经营范围内。

2、投标人不是制造商的，应提供制造商针对本项目的授权。

3、具有良好的商业信誉和健全的财务会计制度，参加政府采购活动前三年内未被列入“信用中国”网站(www.creditchina.gov.cn )失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录名单和“中国政府采购”网站（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单（以递交文件截止当日查询结果为准）。

4、投标人应遵守有关的国家法律、法令、条例和有关招标制度。一旦参加投标，则应承担相关法律责任。

**六、投标截止时间和开标时间：2022**年06月21日10:00 （北京时间）。

投标文件必须在投标截止时间前送达开标地点，并签到（签到地点：四川成都郫县安德镇彭温路399号后勤基建办公区2F评标室），若不签到的投标文件将被拒收，投标人自行承担一切后果。逾期送达或密封和标注不符合招标文件规定的投标文件恕不接受。本次招标不接受邮寄的投标文件。

特别说明：因疫情期间，为保证安全，请前来投标的商家戴好口罩，准备健康二维码，服从学校管理，做好个人防护。

**七、递交投标文件及开标地点**：四川成都郫县安德镇彭温路399号后勤基建办公区2F评标室

**八、联系方式**

采购人：四川铁道职业学院

地址：四川成都郫县安德镇彭温路399号

联系人：贺老师 李老师

联系电话：028-68939969

028-68939919

# 第二章 投标人须知

## 一、投标人须知附表

| 序号 | 应知事项 | 说明和要求 |
| --- | --- | --- |
| 1 | 采购人 | 名称：四川铁道职业学院  地 址：四川成都郫县安德镇彭温路399号  联 系 人：贺老师、李老师  联系电话：028-68939969 68939919 |
| 2 | 项目名称 | 2022年官网三级测评服务 |
| 3 | 招标编号 | TZY-ZB-2022012 |
| 4 | 资金来源 | 财政资金 |
| 5 | 预算金额 | 13.5万元 |
| 6 | 构成招标文件的其他文件 | 招标文件的澄清、修改书及有关补充通知为招标文件的有效组成部分 |
| 7 | 采购方式 | 公开招标 |
| 8 | 评标方法 | 综合评分法 |
| 9 | 投标有效期 | 投标截止之日起30天 |
| 10 | 投标文件份数 | 正本一套，用于唱标的“投标报价表”一份 |
| 11 | 装订要求 | 正本装订，不得有活页 |
| 12 | 投标文件、投标报价表的包装和密封 | 投标文件、“投标报价表”分别包装和密封，同时递交采购人。 |
| 13 | 投标文件递交 | a.时间和地点详见 “投标邀请”;  b.采购人在招标文件规定的时间和地点组织开标，投标人代表人执有效身份证参加。  c.其他要求详见第二章“投标文件”第11条“投标文件的递交”。 |
| 14 | 开标时间、地点 | 时间：2022年 06月21日 10:00（北京时间）  地点：四川成都郫县安德镇彭温路399号后勤基建办公区2F评标室 |

## 二、招标文件

### 1．招标文件的构成

1**.**1本招标文件包括以下内容：

（一）投标邀请；

（二）投标人须知；

（三）投标文件格式；

（四）招标项目技术、商务及其他要求；

（五）评标办法；

（六）合同主要条款；

1**.**2 投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面做出实质性响应是投标人的风险。没有按照招标文件要求作出实质性响应的投标文件将被拒绝。

### 2. 招标文件的澄清和修改

2.1 在投标截止时间前，招标采购单位可以对招标文件进行澄清或者修改。

2.2要求对招标文件进行澄清的投标人，均应通知招标人，招标人应对招标文件进行澄清。

## 三、投标文件

### 3．投标文件的语言

投标人提交的投标文件以及投标人与招标采购单位就有关投标的所有来往书面文件均须使用中文。

### 4. 投标货币

本次招标项目的投标均以人民币报价。

### 5. 知识产权

5.1 投标人应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。

5.2 采购人享有本项目实施过程中产生的知识成果及知识产权。

### 6．投标文件的组成。

投标文件包括：

（1） 投标函

1. 法定代表人授权书
2. 投标报价表
3. 分项报价明细表
4. 商务应答表
5. 投标人近三年类似项目业绩一览表
6. 投标人认为有必要补充说明的相关信息

### 7. 投标文件的说明。

7.1报价部分。投标人按照招标文件要求填写“投标报价表”及“分项报价明细表”。 本次招标报价要求：

（1）投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

（2）投标人每种货物只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

7.2 技术部分。投标人按照招标文件要求做出的技术应答，主要是针对招标项目的技术指标、参数和技术要求做出的实质性响应和满足。投标人的技术应答应包括下列内容：

（1）投标产品的品牌、型号、配置；

（2）投标产品本身的详细的技术指标和参数（尽可能提供检测报告、产品使用说明书、用户手册等材料予以佐证）；

（3）技术方案、项目实施方案；

（4）投标产品技术参数表。

7.3 商务部分。投标人按照招标文件要求提供的有关证明材料及优惠承诺。包括以下内容：

（1）投标函；

（2）法定代表人授权书；

（3）法定代表人和授权代表人身份证复印件；

（4）证明投标人业绩的有关材料；

（5）商务应答表。

### 8．投标文件格式

8.1 投标人应严格按照招标文件第三章中提供的“投标文件格式”填写相关内容。除明确允许投标人可以自行编写的外，投标人不得以“投标文件格式”规定之外的方式填写相关内容。

8.2 对于没有格式要求的投标文件由投标人自行编写。

### 9．投标有效期

投标有效期为开标后 30天。

### 10. 投标文件的密封和标注

10.1 投标人应在投标文件正本封面上注明投标人名称、招标编号、项目名称。

10.2 所有外层密封袋的封口处应粘贴牢固，并加盖密封章（投标人印章）。

10.3 未按以上要求进行密封和标注的投标文件将被拒绝。

### 11．投标文件的递交

11.1投标人应在招标文件规定的投标截止时间前，将投标文件按规定密封后送达开标地点。投标截止时间以后送达的投标文件将被拒绝。

11.2 本次招标不接受邮寄的投标文件。

### 12．投标文件的修改和撤回

12.1 投标人在递交了投标文件后，可以修改或撤回其投标文件，但必须在规定的投标截止时间前，以书面形式通知采购人。

12.2 投标人的修改书或撤回通知书，应由其法定代表人或授权代表签署并盖单位印章。修改书应按招标文件规定进行密封和标注，并在密封袋上标注“修改”字样。

12.3 在投标截止时间之后，投标人不得对其递交的投标文件做任何修改或撤回投标。

12.4 投标文件中如果出现计算上或累加上的算术错误，可按以下原则进行修改：

（1）用数字表示的金额和用文字表示的金额不一致，应以文字表示的金额为准。

（2）单价和数量的乘积与总价不一致时，以单价为准，并修正总价。

（3）单价金额小数点有明显错误的，以总价为准，修正单价。

按上述修正错误的方法调整的投标报价应对投标人具有约束力。如果投标人不接受修正后的价格，其投标将被拒绝。

## 四、开标、评标和中标

**13．开标**

13.1 采购人在招标文件规定的时间和地点组织公开开标，投标人须派代表参加并签到以证明其出席。

13.2 开标时，采购人邀请学校纪检监察室派人对开标及评标全过程进行现场监督。

13.3投标文件中有关明细表内容与“投标报价表”不一致的，以“投标报价表”为准。

### 14．评标

评标采用综合评标法（参见第五章）

### 15．中标通知书

15**.**1 中标通知书为签订采购合同的依据，是合同的有效组成部分。

15.2 中标通知书对采购人和中标人均具有法律效力。中标通知书发出后，采购人改变中标结果，或者中标人无正当理由放弃中标的，应当承担相应的法律责任。

## 五、签订及履行合同和验收

### 16. 签订合同

16.1中标人在收到招标人发出的《中标通知书》后，应在5个工作日内与采购人签订采购合同。由于中标人的原因逾期未与采购人签订采购合同的，将视为放弃中标，采购人有权取消其中标资格并将按相关规定进行处理。

16.2 采购人不得向中标人提出任何不合理的要求，作为签订合同的条件，不得与中标人私下订立背离合同实质性内容的任何协议，所签订的合同不得对招标文件和中标人投标文件作实质性修改。

16.3 中标人因不可抗力原因不能履行采购合同或放弃中标的，采购人可以与排在中标人之后第一位的中标候选人签订采购合同，以此类推。

16.4 中标人在合同签订之后5个工作日内，将签订的合同原件（三份）送采购人。

### 17. 履行合同

17.1 中标人与采购人签订合同后，合同双方应严格执行合同条款，履行合同规定的义务，保证合同的顺利完成。

17.2 在合同履行过程中，如发生合同纠纷，合同双方应按照《合同法》争议解决条款的有关规定进行处理。

### 18. 验收

中标人与采购人按照招标项目技术、商务及其他要求（参见第四章）进行验收，采购人也可依据合同自行组织验收。

## 六、投标纪律要求

### 19. 投标人不得具有的情形

投标人参加投标不得有下列情形：

（1）提供虚假材料谋取中标；

（2）采取不正当手段诋毁、排挤其他投标人；

（3）与招标采购单位、其他投标人恶意串通；

（4）向招标采购单位、采购小组成员行贿或者提供其他不正当利益；

（5）在招标过程中与招标采购单位进行协商谈判；

（6）拒绝有关部门的监督检查或者向监督检查部门提供虚假情况。

有上述情形之一的投标人，属于不合格投标人，其投标或中标资格将被取消。

**七、质疑**

### 20.质疑。

在招标投标过程中，如有任何质疑，可向四川铁道职业学院纪检监察室询问，联系电话：028-68939874。

# 第三章 投标文件格式

## 一、投 标 函

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（采购人名称）：

我方全面研究了 “”项目招标文件（招标编号），决定参加贵单位组织的本项目投标。我方授权（姓名、职务）代表我方（投标单位的名称）全权处理本项目投标的有关事宜。

1. 我方自愿按照招标文件规定的各项要求向采购人提供所需服务，总投标价为

人民币元（大写：）。

2、一旦我方中标，我方将严格履行合同规定的责任和义务，保证于合同签字生效 工作日内完成应尽义务，并交付采购人验收、使用。

3、我方为本项目提交的投标文件正本壹份。

4、我方愿意提供贵公司可能另外要求的，与投标有关的文件资料，并保证我方已提供和将要提供的文件资料是真实、准确的。

5、我方同意本次招标的投标有效期为 。

6、我方完全理解采购人不一定将合同授予最低报价的投标人的行为。

投标人名称： （盖章）

法定代表人或授权代表（签字）：

通讯地址：

邮政编码：

联系电话：

传 真：

日 期：

## 二、法定代表人授权书

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（采购人名称）：

本授权声明：（投标人名称）（法定代表人姓名、职务）授权（被授权人姓名、职务）为我方 “ ” 项目（招标编号）投标活动的合法代表，以我方名义全权处理该项目有关投标、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人签字：

授权代表签字：

投标人名称： （盖章）

日 期：

## 三、投标报价表

投标人名称： 招标编号：

|  |  |
| --- | --- |
| 项目名称 |  |
| 投标总价 | （大写）人民币  （小写）￥： |
| 供货周期 |  |
| 备 注 |  |

投标人代表签字：

（盖公章）

日期：年月日

## 四、分项报价明细表

招标编号：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 规格型号 | 品牌 | 单位 | 数量 | 单价 | 金额 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 分项报价合计（万元） | | | | | |  |  |

注：

1、投标人必须按“分项报价明细表”的格式详细报出投标总价的各个组成部分的报价并具体填写品牌、规格、型号等，否则作无效投标处理。如产品为国家节能、环保标志清单产品也请在备注栏注明。

2、“分项报价明细表”各分项报价合计应当与“投标报价表”报价合计相等。

投标人名称： （盖章）

法定代表人或授权代表（签字）：

投标日期：

## 五、商务应答表

招标编号：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件要求 | 投标文件应答 | 偏离及其影响 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：

供应商必须据实填写，不得虚假应答，否则将取消其投标或中标资格。

投标人名称： （盖章）

法定代表人或授权代表（签字）：

投标日期:

## 六、投标人近三年类似项目业绩一览表

招标编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 年份 | 用户名称 | 项目名称 | 完成时间 | 合同金额 | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

投标人以上业绩需提供有关书面证明材料（中标通知/合同复印件，原件备查，规格型号、数量、价格等具体内容不能遮盖，否则投标无效）。如要求描述“完成项目质量”，则需提供合同验收合格或用户单位书面证明，表不够可另附。

投标人名称： （盖章）

法定代表人或授权代表（签字）：

投标日期:

## 七、投标人最近三年经审计的财务报告

（格式自拟）

## 八、投标人最近一年任意一月的税收和社会保障金证明

（格式自拟）

## 九、投标人认为有必要补充说明的相关信息

（格式自拟）

# 第四章 招标项目技术、商务及其他要求

|  |  |
| --- | --- |
| 项目名称 | 官网三级保护测评 |
| 详细技术参数  （包括：规格、型号、数量、技术要求和售后服务要求等） | **（一）项目概述：**  为了落实公安部、网信办以及教育厅对高校应用系统安全等级保护要求，进一步增强系统安全防护能力，确保系统安全稳定运行，防止因系统安全事件引发安全事故依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全等级保护管理办法》（公通字[2007]43号）和《中华人民共和国网络安全法》等标准规范，四川铁道职业学校现拟招一家供应商提供等保测评服务。  本项目测评的对象：   |  |  | | --- | --- | | 系统名称 | 安全等级 | | 四川铁道职业学院官网 | 三级 |   项目目标:  依据国家和行业信息安全的相关标准，全面了解和掌握系统现有安全状况，找出其与《网络安全等级保护基本要求（GBT22239-2019）》对应级别的差距，及时发现系统存在的安全问题；针对等级保护测评中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。有效提升目标系统及其所在核心网络抵御物理损害、恶意攻击的能力。  项目依据：  此次依据的标准包括但不限于以下内容：  1）《信息安全等级保护管理办法》（公通字[2007]43号）  2）《信息安全技术信息系统安全等级保护基本要求》GB/T 22239-2019  3）《信息安全技术信息系统安全等级保护定级指南》GB/T 22240-2008  4）《信息安全技术信息系统安全等级保护实施指南》GB/T 25058-2010  5）《信息安全技术信息安全风险评估规范》GB/T 20984-2007  6）《信息安全技术信息系统安全等级保护测评要求》GB/T 28448-2019  7）《信息安全技术信息系统安全等级保护测评过程指南》GB/T 8449-2018  8）《中华人民共和国网络安全法》  **（二）项目技术参数要求**  1.测评要求  根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：   | **序号** | **关键实施阶段** | **工作要求** | | --- | --- | --- | | 1 | 确定测评范围 | 明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。 | | 2 | 获得信息系统的信息 | 通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。 | | 3 | 确定具体的测评对象 | 初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。 | | 4 | 确定测评工作的方法 | 根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。 | | 5 | 制定测评工作计划 | 制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。 | | 6 | 实施等级保护测评 | 实施测评，包括人工检查、工具扫描等方式。 | | 7 | 项目总结 | 对测评结果进行总结、汇报 |   2.测评内容  按照网络安全等级保护测评依据开展测评工作（包括不限于以下项目）：  （1）安全物理环境  安全物理环境检查主要是了解信息系统的物理安全保障情况，涉及对象为机房。在内容上，安全物理环境层面测评实施过程涉及的工作单元，具体如下表：  表1 安全物理环境测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 物理位置的选择 | 检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 | | 2 | 物理访问控制 | 检查机房出入口等过程，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 | 检查机房内的主要设备、介质和防盗报警设施等过程，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 | 检查机房设计/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 | 检查机房防火方面的安全管理制度，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 | 检查机房及其除潮设备等过程，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 | 检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 | | 8 | 温湿度控制 | 检查机房的温湿度自动调节系统，测评信息系统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 | 检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 | | 10 | 电磁防护 | 检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |   （2）安全通信网络  安全通信网络检查主要是了解系统的网络架构和通信传输等，涉及对象为防火墙、核心路由器、核心交换机等设备和网络架构。在内容上，安全通信网络层面测评过程涉及的工作单元，具体如下表：  表2 安全通信网络测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 网络架构 | 检查核心设备的CPU和内存使用率，整个网络带宽是否满足现状，VLAN划分是否合理，网络架构是否做到设备冗余、链路。 | | 2 | 通信传输 | 检查数据在传输过程中的的完整性和保密性措施。 | | 3 | 可信计算 | 检查设备是否进行可信验证。 |   （3）安全区域边界  安全区域边界检查主要是了解系统在网络边界的防护措施，涉及对象为防火墙、入侵检测、安全审计等安全设备。在内容上，安全区域边界层面测评实施过程涉及的工作单元，具体如下表：  表3 安全区域边界测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 边界防护 | 检查网络边界是否有访问控制设备，访问控制策略是否合理，是否关闭了闲置端口等。 | | 2 | 访问控制 | 检查网络中的访问控制策略是否合理、有效。 | | 3 | 入侵防范 | 检查网络中是否采用了入侵防范措施，验证该措施是否有效。 | | 4 | 恶意代码和垃圾邮件防范 | 检查网络中是否有恶意代码和垃圾邮件防范措施。 | | 5 | 安全审计 | 检查网络中是否有综合安全审计措施。 | | 6 | 可信验证 | 检查设备是否进行可信验证。 |   （4）安全计算环境  安全计算环境检查主要是了解系统的运行环境是否采取了相关安全措施，涉及对象为网络设备、安全设备、操作系统、数据库、中间件等。在内容上，安全计算环境层面测评实施过程涉及的工作单元，具体如下表：  表4应用系统安全测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 身份鉴别 | 检查所有设备的登录用户是否有身份鉴别措施，是否有复杂度、唯一性等检查。 | | 2 | 访问控制 | 检查用户的权限分配情况，默认用户和默认口令使用情况等。 | | 3 | 安全审计 | 检查是否开启安全审计功能，是否能审计到每个用户，审计记录是否有保护措施。 | | 4 | 入侵防范 | 检查设备在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 | | 5 | 恶意代码防范 | 检查设备的恶意代码防范情况。 | | 6 | 可信验证 | 检查设备是否进行可信验证。 | | 7 | 数据完整性 | 检查系统数据的传输完整性和存储完整性措施。 | | 8 | 数据保密性 | 检查系统数据的传输保密性和存储保密性措施。 | | 9 | 数据备份恢复 | 检查系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 | | 10 | 剩余信息保护 | 检查系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。 | | 11 | 个人信息保护 | 检查系统对个人信息的采集和使用情况。 |   （5）安全管理中心  安全管理中心检查主要是了解系统在管理、审计等集中管理的情况，涉及对象为综合管理类设备、综合审计类设备等。在内容上，安全管理中心实施过程涉及的工作单元，具体如下表：  表5安全管理中心测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 系统管理 | 检查是否对系统管理员进行统一的身份鉴别，操作审计等。 | | 2 | 审计管理 | 检查是否对审计管理员进行统一的身份鉴别，操作审计等。 | | 3 | 安全管理 | 检查是否对安全管理员进行统一的身份鉴别，操作审计等。 | | 4 | 集中管控 | 检查是否划分独立的安全管理区域，是否对网络中运行的设备进行状态监测、日志审计、安全审计等，是否对补丁、恶意代代码进行统一管理。 |   （6）安全管理制度  安全管理制度测评是为了了解评测安全管理制度的制定、发布、评审和修订等情况，主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及的工作单元，具体如下表：  表6安全管理制度测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 安全策略 | 核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目 标、范围、原则和各类安全策略 | | 2 | 管理制度 | 检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。 | | 3 | 制定和发布 | 检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 | | 4 | 评审和修订 | 检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |   （7）安全管理机构  安全管理机构测评是为了了解评测安全管理机构的组成情况和机构工作组织情况，主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。在内容上，安全管理机构测评实施过程涉及的工作单元，具体如下表：  表7安全管理机构测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 岗位设置 | 检查部门/岗位职责文件，测评信息系统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 | 检查人员名单等文档，测评信息系统各个岗位人员配备情况。 | | 3 | 授权和审批 | 检查相关文档，测评信息系统对关键活动的授权和审批情况。 | | 4 | 沟通和合作 | 检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。 | | 5 | 审核和检查 | 检查记录文档等过程，测评信息系统安全工作的审核和检查情况。 |   （8）安全管理人员  安全管理人员测评是为了了解单位人员安全方面的情况，主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。在内容上，安全管理人员测评实施过程涉及的工作单元，具体如下表：  表8安全管理人员测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 人员录用 | 检查人员录用文档等过程，测评信息系统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 | 检查人员离岗安全处理记录等过程，测评信息系统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 | 检查培训计划和执行记录等文档，测评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 | 检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |   （9）安全建设管理  安全建设管理测评是为了了解评测系统建设管理过程中的安全控制情况，主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全建设管理测评实施过程涉及的工作单元，具体如下表：  表9安全建设管理测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 定级和备案 | 检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。 | | 2 | 安全方案设计 | 检查系统安全建设方案等文档，测评系统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 | 测评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 | 检查相关软件开发文档等，测评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 | 检查相关文档，测评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 | 检查相关文档，测评系统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 | 检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。 | | 8 | 系统交付 | 检查系统交付清单等过程，测评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 | 检查系统之前等级测评的情况，以及之前测评机构的资质等。 | | 10 | 服务供应商选择 | 测评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  安全运维管理测评是为了了解系统运维管理过程中的安全控制情况，主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全运维管理测评实施过程涉及的工作单元，具体如下表：  表10安全运维管理测评内容   |  |  |  | | --- | --- | --- | | **序号** | **工作单元名称** | **工作单元描述** | | 1 | 环境管理 | 检查机房安全管理制度，机房和办公环境等过程，测评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 | 检查资产清单，检查系统、网络设备等过程，测评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 | 检查介质管理记录和各类介质等过程，测评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 | 检查设备使用管理文档和设备操作规程等过程，测评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 | 检查系统对于漏洞和安全隐患风险的管理，是否有报告、记录等文档，是否定期开展安全测评等。 | | 6 | 网络和系统安全管理 | 检查系统和网络的安全管理文档，是否明确了角色划分、权限划分，是否覆盖安全策略、账户管理、配置文件的生成及备份、变更审批等内容；检查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修 改等内容；核查是否具有对日志、监测和报警数据等进行分析统计的报告；核查开通远程运维的审批记录，核查针对远程运维的审计日志是否不可以更改等。 | | 7 | 恶意代码防范管理 | 检查恶意代码防范管理文档和恶意代码检测记录等过程，测评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 | 检查是否对基本配置信息进行记录和保存，基本配置信息改变后是否及时更新基本配置信息库等。 | | 9 | 密码管理 | 测评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 | 检查变更方案和变更管理制度等过程，测评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 | 检查系统备份管理文档和记录等过程，测评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 | 资产管理 | 检查是否有资产清单，清单是否包括资产类别、资产责任部门、 重要程度和所处位置等内容；是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施 的选取上是否不同；核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。 | | 13 | 应急预案管理 | 检查应急响应预案文档等过程，测评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 | 检查外包运维服务情况，单位是否符合国家有关规定，协议是否明确约定外包运维的范围和工作内容等。 |   3.交付产物  包括但不仅限于以下资料：  （1）★信息系统安全等级测评报告（包含整改建议）  （2）公安机关要求的、其他未列入的相关资料 |
| 项目其他需求 | **项目技术、服务要求**  （1）服务时间: 合同签订之日起至取得公安部门颁发的《信息系统安全等级保护备案证明》。  （2）服务地点: 四川铁道职业学院。  （3）自合同签订之日起，提供一年7\*24小时等级保护和网络安全咨询服务。 |
| 验收内容及标准 | 验收内容：  完整有效的测评目标的等级测评报告、信息系统安全整改建议报告，公安机关通过相关的等级保护备案审查。  验收标准：  （1）等级测评报告通过公安机关审核。若不能达到审核标准，须指导学校进行安全整改，并重新完成测评，直至取通过审核。  （2）信息系统安全整改建议报告在符合学校实际情况的条件下，详细完整，可实际操作。  （3）取得纸质版《信息系统安全等级保护备案证明》。  （4）存在国家强制规定或行业标准的遵照相关规定执行。 |

# 第五章 评标办法

一、评标办法

本次评标采用综合评标法。

二、评分办法说明

对各投标文件采取综合评分法进行详细评审，满分为 100 分，招标主要考评因素包括综合投标报价（10%）、测评方案响应性（10%）、专业人员技术力量(48%)、履约能力（30%）、文件规范（2%）五个方面，各投标人各方面的所有评价指标的得分之和就是该投标人的综合得分。

详细评分标准如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素及权重 | 分值 | 评分标准 | 说明 |
| **一** | **价格10%** | **10** | 1.经评标委员会评审，通过资格性和符合性审查，且投标报价最低的投标人的投标报价作为评标基准价；  2.投标报价得分=(评标基准价／投标报价)×10 |  |
| **二** | **测评方案响应性10%** | | | |
| 1 | 测评方案 | 10 | 1.等保测评方案中包含测评流程、测评方法、测评指标和配合需求；每项内容满足本项目实际需求的得1分，缺少或不满足本项目实际需求不得分，本项最多得4分；  2.等保测评方案正确理解网络安全等级测评，测评思路清晰、测评内容完整、测评重点突出，测评方案包括但不限于：①项目实施标准；②方案编制；③现场测评；④报告编制；⑤项目人员安排；⑥项目实施周期等内容进行综合评审，以上内容详尽、完整且具有针对性得6分，每缺少一项或不完善扣1分，扣完为止； |  |
| **三** | **专业人员技术力量48%** | | | |
| 1 | 投标人机构技术团队情况 | 15 | 技术负责人同时具有:  1.信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书；  2.注册信息安全专业人员（CISP）证书；  3.注册云安全系统认证专家（CCSSP）证书；  4.信息安全测评师；  5.具有高级及以上职称证书；  6.网络与信息安全应急人员（管理I级）；  以上证书，每提供一个得2.5分，最多得15分，未提供不得分。 | 以上人员提供2020年连续3个月的社保材料。 |
| 2 | 18 | 项目经理同时具有：  1.信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书；  2.信息安全测评师；  3.注册云安全系统认证专家（CCSSP）证书；  4.网络与信息安全应急人员（管理I级）；  5.信息安全保障人员（CISAW）（认证方向：应急服务）；  6.计算机软件产品检验员证书。  以上证书，每提供一个得2.5分，最多得15分，未提供不得分。  获得过国家信息安全等级保护工作协调小组办公室颁发的个人荣誉证书的得3分。 |
| 3 | 15 | 测试团队人员（不包含技术负责人、项目经理）在具有信息安全等级测评师证书的同时具有以下证书：  1.信息安全等级评测师证书或网络安全等级评测师证书；  2.网络与信息安全应急人员（技术I级）；  3.注册网络安全专业防御人员（NSATP-D）；  4.计算机技术与软件专业技术资格（信息安全工程师）证书；  5.信息安全保障人员（CISAW）（认证方向：工控网络安全）；  6.注册云安全系统认证专家（CCSSP）证书。  以上证书，每提供一个得2.5分，最多得15分，未提供不得分。 |
| **四** | **履约能力30%** | | | |
| 1 | 投标人  业绩 | 10 | 2020年1月1日以来，具有信息安全测评项目案例，每具有1个合同得2分，最多得10分； | 附有效证明文件复印件（加盖投标人公章，原件备查）。 |
| 2 | 投标人机构情况 | 20 | 1.具有质量管理体系认证证书,认证范围包括“评估测试服务”得2分；  2.具有信息技术服务管理体系证书,认证范围包括“评估测试服务”得2分；  2.具有信息安全管理体系证书,认证范围包括“评估测试服务”得2分；  3.投标人具有工业信息安全应急服务支撑单位证书得4分，具有工业信息安全测试评估机构能力认定证书得4分，未提供相关证明材料的不得分；  4.投标人在2018年至今，具有一份及以上CNVD颁发的“原创漏洞证明”证书，一个得0.5分，最高得6分。 |
| **五** | **文件规范性 2分** | | | |
|  | 投标文件规范 | 2 | 投标文件制作规范，没有细微偏差情形的得2分；有一项细微偏差扣0.2分，扣完为止。 |  |

# 第六章 合同主要条款

系统安全等级测评服务合同

甲方：

乙方：

依照《中华人民共和国民法典》及其他有关法律、行政法规、遵循自愿、公平和诚实信用的原则，双方就本项目测评事项协商一致，订立本合同。

受甲方委托，由乙方根据测评范围对甲方的××××系统（以下简称：本系统）进行等级保护测评。为保证测评过程的顺利进行，现经甲、乙双方平等协商，自愿签订本协议，共同遵守如下条款：

1．服务范围

测评服务：乙方依据《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》、《中华人民共和国网络安全法》等有关规定及要求，并且甲方本系统在公安机关获取到系统备案证书或备案证号后,开展符合性等级保护测评工作。

工作内容：根据《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》、《中华人民共和国网络安全法》等有关规定及要求，对本系统进行第三方测评工作，为保证测评的真实性，乙方将客观、公正的对系统开展评估工作，在评估过程中出现的不符合性，乙方将如实反馈并提出相应整改建议，甲方自行开展整改工作。乙方根据甲方实际整改情况出具（优/良/中/差）结论的测评报告。

测评时间要求：

若合同签订时间迟于甲方取得备案证时间，则在合同签订后XX个工作日内乙方完成甲方指定系统的预评估；反之，乙方在甲方取得备案证后XX个工作日完成系统预评估工作。

根据预评估结果，若甲方系统无高风险项并综合评估达到70分以上含70分，乙方在XX个工作日内完成正式测评工作并出具《网络安全等级保护测评报告》（结果为：优、良、中）。若甲方系统存在高风险项并综合评估未能达到GB/T 22239-2019中第2或3级系统的要求，乙方在XX个工作日内出具整改建议；甲方整改完成后3个工作日内通知乙方进场开展正式测评工作，根据公安机关相关要求及规定，本次测评无论测评结论如何，乙方将如实出具《网络安全等级保护测评报告》。

3.付款方式

合同总额为人民币：￥ 元（大写： 万元整）；

乙方应向甲方提交相应金额的增值税发票（服务类：6%）。

合同首付款：甲方应在与乙方签订合同后5个工作日内支付合同总额50%，即：人民币： ￥ 元（大写： 万元整）；

甲方应在乙方完成预测评后5个工作日内支付合同总额40%，即：人民币：￥ 元（大写： 万元整）；

甲方应在乙方完成测评工作且提交了《网络安全等级保护测评报告》后5个工作日内支付合同总额10%，即：人民币：￥ 元（大写： 万元整）。

5．保证条款

1） 乙方保证在为甲方提供服务过程中所使用的产品、资料、技术不涉及任何第三方利益、不侵犯任何第三方的知识产权和其他权益，且不存在任何与此相关的争议，若乙方违反上述保证给甲方造成损失，乙方应负责赔偿。

2） 甲方、乙方依照本合同约定解除合同或本合同履行完毕后，本保证条款仍然有效，不受本合同期限的限制。

6．保密条款

1） 本条所称“商业秘密”指甲、乙双方各自所拥有的，不为公众所知的管理信息、方式方法、客户信息、商业数据、产品信息、销售渠道、技术诀窍等，或由甲、乙双方在履行本合同过程中明确为商业秘密的或为法律所认可的任何信息。

2） 在本合同履行期内，获取对方商业秘密的一方仅可将该商业秘密用于履行其在本合同项下的义务，且只能由相关的工程技术人员使用。获取对方商业秘密的一方应当采取适当有效的方式保护所获取的商业秘密，不得未经授权使用、传播或公开商业秘密。本合同终止后，一方应立即归还从对方处获得的一切保密信息（测评记录除外），或以对方认可的方式进行销毁。

3） 乙方有义务对甲方提交的任何文档资料以及检测评估数据与结果保密，严格依照《中华人民共和国保密法》相关内容执行，以确保任何相关技术及业务文档不得泄露。未经甲方同意，严禁将任何相关技术及业务文档向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。

4） 甲方、乙方依照本合同约定解除合同或本合同履行完毕后，本保密条款仍然有效，保密信息接收方仍应承担保密义务。

7．违约责任

甲方如未按合同要求及时提供相应协作支持，造成项目工期延误或评估服务异常终止，甲方应承担相应责任。甲方所承担的责任以甲方应支付的服务费为限。造成乙方增加评测工作量及人员投入的，双方应协商适当追加服务费用。

乙方如因自身原因逾期提交《网络安全等级保护测评报告》的（因不可抗力或甲方原因造成逾期的除外）,双方应协商后，乙方向甲方支付适当的违约金。

如任何一方无故单方面解除合同，应向对方支付合同金额30%的违约金。

8．纠纷解决

凡因本合同引起的或与本合同有关的任何争议，双方同意以诚信的态度协商解决。30天内仍协商不成的，依法向甲方所在地人民法院起诉。

9．合同生效、终止

1) 本合同一经签署，未经双方同意，任何一方不得随意更改。本合同所列的附件为本合同不可分割的组成部分，与本合同具有同等的法律效力。如本合同在履行过程中有任何变更、补充或修改，双方应另行签订书面协议。

2) 如发生以下情况，任何一方有权终止合同，但须以书面形式通知对方：

一方进入破产、撤销或已进入清算阶段，或被解散、被依法关闭；一方财务状况严重恶化，不能支付到期债务；出现了本合同规定的或法定解除事由。

3） 本合同共 页，一式 （中文大写）份具有同等法律效力，甲方执 份，乙方执 份。本合同经双方签字盖章后生效，未尽事宜双方友好协商解决。

以上合同内容仅做参考，以实际签订为准。