|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 询价采购文件

|  |  |
| --- | --- |
| **项目名称：** | **恩施机场网络安全等级保护测评服务采购项目** |

|  |  |
| --- | --- |
| **采 购 单位：** | **湖北机场集团恩施机场有责任公司** |
| **编制时间：** | **2025年09月30日** |

 |

目 录

第一章 询价函 1

第二章 询价评议 3

一、询价方法 3

二、询价步骤 3

三、确定成交供应商办法（最低价法） 4

四．询价响应文件的数量和签署 4

六、签订合同 5

七、询价采购失败条件 5

八、 其他 5

第三章 采购项目内容及技术规格要求 6

一、采购清单 6

二、定检维保内容 6

三、商务要求 19

四、附《湖北机场集团有限公司“供应商不良行为”管理办法》 20

第四章 询价响应文件格式 23

第五章 采购合同 30

# 第一章 询价函

湖北机场集团恩施机场有限责任公司对“恩施机场网络安全等级保护测评服务采购项目”进行询价采购，欢迎符合资格条件的供应商参与询价。

**一、项目概况**

1、项目名称：恩施机场网络安全等级保护测评服务采购项目

2、最高限价：8万元，供应商报价不得超过最高限价，否则其报价无效。

3、采购需求：完成恩施机场三级等级保护系统（安检信息系统）的等级保护测评工作；完成恩施机场当地公安机关的网络安全等级保护登记、备案等工作。具体详见第三章采购项目内容及技术规格要求。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务内容** | **服务地点** | **测评期限** | **备注** |
| 1 | 恩施机场网络安全等级保护测评服务 | 恩施机场 | 合同签订后35个日历天内，完成等级保护测评工作，45个日历天内取得当地公安机关备案回执 |  |

4、询价有效期：自询价之日起60个日历天。

**二、供应商资格要求**

1、供应商须在中华人民共和国市场监督管理部门注册，具有独立法人资格和有效的营业执照；

2、供应商须具有公安部第三研究所颁发的有效《网络安全等级测评与检测评估机构服务认证证书》。

3、供应商未被列入“信用中国”网站(www.creditchina.gov.cn)或者“中国执行信息公开网”（zxgk.court.gov.cn）失信被执行人名单（提供网站查询截图）；

4、供应商需对关《湖北机场集团有限公司“供应商不良行为”管理办法》在“第六章 询价响应文件格式”“资格证明材料”中做出承诺，承诺格式详见询价响应文件格式；

5、本项目不接受联合体响应。

**以上资格要求为本次项目供应商应具备的基本条件，参加报名、报价的供应商必须满足资格要求中的所有条款，并按照询价文件规定在响应文件中递交资格证明文件。**

**三、询价文件获取地点、响应递交截止时间及地点**

1、询价文件获取地点：恩施机场公司官网本项目公告附件中直接下载。

2、响应文件递交截止时间：2025年10月14日09时30分（北京时间，法定节假日除外）。

3、响应文件递交地点：恩施许家坪国际机场行政楼111办公室。

**四、联系方式**

名    称：湖北机场集团恩施机场有限责任公司

地    址：恩施许家坪国际机场

联 系 人：王蒙

电 话：18671816956

**五、信息发布媒体**

恩施机场公司官网、湖北机场集团内外网。

湖北机场集团恩施机场有限责任公司

2025年09月30日

# 第二章 询价评议

一、询价方法

1.1询价小组：询价小组成员由三人组成。

1.2监督：由监管部门相关人员现场监督。

1.3询价评议：询价小组负责对供应商递交询价响应文件的有效性、完整性和对询价响应文件的响应程度进行符合性审查、商务评议和技术评议。

二、询价步骤

2.1响应文件开启

2.1.1采购人在第一章“询价公告”中约定的日期、时间和地点组织询价响应文件公开开启，**供应商只需在响应文件递交截止时间前现场递交或邮寄（收件人：王蒙，18671816956，湖北省恩施市许家坪路38号恩施许家坪国际机场行政楼111办公室）送达响应文件，邮寄的响应文件供应商应确保在递交截止时间前送达**。

2.1.2开启程序

（1）公布在递交响应文件截止时间前响应文件的递交情况，并由监督人员检验供应商响应文件的密封性；

（2）开启结束。

2.2审查及评议

2.2.1询价小组审查各供应商的询价响应文件是否实质上响应了询价通知书的要求。实质上响应的询价响应文件应该是与询价通知书要求的全部条款、条件和规格相符，响应文件不允许偏离采购内容的技术参数。

2.2.2在递交询价响应文件截止时间后，供应商不得通过修正或撤销不合要求的偏离或保留从而使其报价成为实质上响应的报价。

2.2.3资格审查要求见第一章 询价函供应商资格要求。

2.2.4符合性审查中发现下列情况之一的，其询价响应文件将被视为未实质性响应询价文件，而作无效报价处理：

1）未按询价文件要求签署、盖章；

2）报价超限价，存在缺项、漏项；出现两个及以上不同报价或响应方案；

3）响应有效期不符合采购文件要求；

4）交货期（工期/服务期）、质保期不符合询价文件要求；

5）不满足询价文件技术、服务及商务等实质性要求；

6）有围标串标情况。

2.3询价响应文件的澄清。

在评审期间，询价小组可要求供应商对其询价响应文件中含义不明确、对同类问题表述不一致或有明显文字和计算错误的内容做必要的澄清，说明或者补正。供应商有责任按照采购人的通知指派专人进行答疑和澄清，但澄清、说明或者补正不得超出询价响应文件的范围或者改变询价响应文件的实质性内容。澄清回复均应由供应商的法定代表人或授权代表签字的书面形式作出。

三、确定成交供应商办法（最低价法）

3.1询价小组从质量和服务均能满足采购文件实质性响应要求的供应商中，按照报价由低到高的顺序推荐3名（不足3名的按实际数量推荐）成交候选人，并编写评审报告。

3.2如果有两家或两家以上供应商的报价相同，由询价小组对各供应商的技术、服务等因素做出评价来确定一家供应商作为第一成交候选人；如果两家或两家以上供应商的报价和技术、服务都相等，由询价小组集体采用随机抽取或投票的方式确定一家供应商作为第一成交候选人。

3.3采购人根据询价小组的成交候选供应商名单，根据质量和服务均能满足询价通知书实质性响应要求且报价最低的原则确定成交供应商。

四．询价响应文件的数量和签署

4.1供应商应编制响应文件一式三份,其中正本一份和副本二份，供应商的副本可采用正本的复印件。每套投标文件须清楚地标明“正本”、“副本”。若副本与正本不符，以正本为准。

4.2响应文件的正本需打印或用不褪色墨水书写,并由法定代表人或经其正式授权的代表在相应位置处签字。授权代表须将以书面形式出具证明，其《法定代表人授权书》应附在响应文件中。

五、响应文件的递交

5.1为方便授权代表身份核验，《法定代表人授权书》除在询价响应文件中提供之外，另需单独准备一份，无需密封，便于在递交响应文件时手持验证身份（同时需准备身份证原件或电子身份证）。

5.2为方便评审核验报价，《报价一览表》除在询价响应文件中提供之外，需单独一份密封提交，并在信封上标明“投标一览表”字样。

5.2响应文件一式三份,其中正本一份和副本二份应合封一个包密封提交。

5.3所有信封均应注明供应商名称、项目名称、项目编号（如有）、供应商地址、联系人、电话和有“在（响应文件中规定的开标日期和时间）之前不得启封”的字样，封口处加盖投标人印章（样式附后）。

|  |
| --- |
| **项目名称：****项目编号：****供应商名称：****供应商地址、联系人、电话****在规定的开标时间****年 月 日 时 分之前不得启封** |

5.4如果未按要求密封和标记，采购人将拒绝接受供应商的响应文件。

六、签订合同

6.1成交供应商在收到成交通知书后，按其规定与采购人签订合同。

七、询价采购失败条件

7.1出现影响采购公正的违法、违规行为的；

7.2因重大变故，采购任务取消的；

7.3有效报价供应商不满足法定家；数的

7.4所有报价均超过采购预算的。

**八、**其他

8.1本文件最终解释权归采购人所有。

# 第三章 采购项目内容及技术规格要求

## 一、采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务内容** | **服务地点** | **测评期限** | **备注** |
| 1 | 恩施机场网络安全等级保护测评服务 | 恩施机场 | 合同签订后35个日历天内，完成等级保护测评工作，45个日历天内取得当地公安机关备案回执 |  |

## 二、技术、服务要求

（一）项目概况：依据《信息安全等级保护管理办法》第十四条规定，信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构；依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。三级信息系统应当每年至少进行一次等级测评。本机场三级系统（安检信息系统）备案有效期至2025年10月31日，现需采购一家测评机构对本机场进行年度测评。

（二）技术要求：根据国家《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）、《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）、《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术 网络安全等级保护过程指南》（GB/T28449-2018）及《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）及等文件精神对信息系统的各项要求对系统进行等级保护测评。协助采购方进行系统定级、备案工作。完成对平台的安全等级保护测评工作，指导采购方对系统测评中提出的不符合项进行整改，提出安全整改建议，编制整改方案。最终出具符合要求的安全等级保护测评报告，协助采购方取得公安机关颁发的备案证明。评估机构应具有攻防演练实验室平台，可提供高效、精准的信息安全风险检测结果。

（三）第三级系统测评内容：

**1.安全物理环境**

测评对象主要为主机房，涉及工作单元10个，具体如下表：

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 物理访问控制 | 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 |
| 3 | 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。 |
| c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。 |
| 4 | 防雷击 | a) 应将各类机柜、设施和设备等通过接地系统安全接地。 |
| b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 |
| 5 | 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。 |
| c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 |
| 6 | 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。 |
| c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 |
| 7 | 防静电 | a) 应采用防静电地板或地面并采用必要的接地防静电措施。 |
| b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 |
| 8 | 温湿度控制 | a) 应设置温、湿度自动询节设施，使机房温、湿度的变化在设备运行所允许的范围之内。 |
| 9 | 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。 |
| c) 应设置冗余或并行的电力电缆线路为计算机系统供电。 |
| 10 | 电磁防护 | a) 电源线和通信线缆应隔离铺设，避免互相干扰。 |
| b) 应对关键设备实施电磁屏蔽。 |

**2.安全通信网络**

测评对象主要为网络互联设备、网络安全设备以及网络拓扑结构等三大类，具体为：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，信息系统的整体网络拓扑结构，提供可信验证的设备或组件、提供集中审计功能的系统；涉及工作单元3个，具体如下表：

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 网络架构 | a) 应保证网络设备的业务处理能力满足业务高峰期需要。 |
| b) 应保证网络各个部分的带宽满足业务高峰期需要。 |
| c) 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。 |
| d) 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。 |
| e)应提供通信线路板、关健网络设备和关键计算设备的硬件冗余，保证系统的可用性。 |
| 2 | 通信传输 | a)应采用校验技术或密码技术保证通信过程中数据的完整性  |
| b)应采用密码技术保证通信过程中数据的保密性 |
| 3 | 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、重要配登参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，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。 |

**3.安全区域边界**

测评对象主要为：网闸、防火墙、路由器、交换机和无线接入网关设备、抗ATP攻击系统、网络回溯系统、抗DDOS攻击系统、入侵保护系统、入侵检测系统、防病毒网关和UTM、综合安全审计系统、提供可信验证的设备或组件、提供集中审计功能的系统。涉及工作单元6个，具体如下表：

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 边界防护 | a) 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。 |
| b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制。 |
| c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制。 |
| d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 |
| 2 | 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。 |
| e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |
| 3 | 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。 |
| d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重 入侵事件时应提供报警。 |
| 4 | 恶意代码和垃圾邮件防范 | a）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。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级 和更新。 |
| 5 | 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。 |
| d）应能对远程访问的用户行为、访问物联网的用户行为等单独进行行为审计和数据分析 |
| 6 | 可信验证 | 可信验证 可基于可信针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进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将其验证结果形成审计记录并送至安全管理中心。  |

**4.安全计算环境**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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。 |
| d)应采用口令、密码技术、生物技术等两种或两种以上组合术来实现。 |
| 2 | 访问控制 | a)应对登陆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。 |
| e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则 |
| f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。 |
| g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 |
| 3 | 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)应对设计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| d)应对审计进程进行保护，防止未经授权的中断 |
| 4 | 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。 |
| f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 |
| 5 | 恶意代码防范 | 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断 |
| 6 | 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。 |
| 7 | 数据完整性 | a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、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。 |
| b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、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 | a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限千鉴别数据、重要业务数据和重要个人信息等。 |
| b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 |
| 9 | 数据备份和恢复 | 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。 |
| 10 | 剩余信息保护 | a)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。 |
| b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 |
| 11 | 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。 |

**5.安全管理中心**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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、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。 |
| 2 | 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。 |
| 3 | 安全管理 | a) 应对安全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管理操作，并对这些操作进行审计。 |
| b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统 一 安全标记，对主体进行授权，配置可信验证策略等。 |
| 4 | 集中管控 | a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。 |
| b) 应能够建立 一 条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。 |
| c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。 |
| d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。 |
| e) 应对安全策略，恶意代码，补了升级等安全相关事项进行集中管理 |
| f) 应能对网络中发生的各类安全事件进行识别、报警和分析。 |

**6.安全管理制度**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 |
| 3 | 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。 |

**7.安全管理机构**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 岗位设置 | a) 应成立指导和网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。 |
| b) 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。 |
| c) 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。 |
| 2 | 人员配备 | a) 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。 |
| b) 应配备专职安全管理员，不可兼任。 |
| 3 | 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建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。 |
| c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 |
| 4 | 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。 |
| 5 | 审核和检查 | a)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。 |
| b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。 |
| c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 |

**8.安全管理人员**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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，对其所具有的技术技能进行考核。 |
| c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 |
| 2 | 人员离岗 | a) 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。 |
| b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 |
| 3 | 安全意识教育和培训 | a) 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。 |
| b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。 |
| c) 应定期对不同岗位的人员进行技能考核 |
| d)应对安全教育和培训的情况和结果进行记录并归档保存。 |
| 4 | 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。 |
| d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 |

**9.安全建设管理**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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公安机关备案。 |
| 2 | 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及与其他级别保护对象的关系进行安全整体规划 和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件 |
| c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性 进行论证和审定，经过批准后才能正式实施。 |
| 3 | 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主管部门的要求。 |
| c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品 名单 |
| 4 | 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) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则 |
| c) 应制定代码编写安全规范，要求开发人员参照规范编写代码 |
| d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制 |
| e) 应保证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 |
| f)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制 |
| g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查 |
| 5 | 外包软件开发 | a) 应在软件交付前检测软件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 |
| c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道 |
| 6 | 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 |
| c) 应通过第三方工程监理控制项目的实施过程 |
| 7 | 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，安全测试报告应包含密码应用 安全性测试相关内容 |
| 8 | 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 |
| 9 | 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同家有关规定 |
| 10 | 服务供应商管理 | 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 |
| c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制 |

**10.安全运维管理**

| **序号** | **工作单元名称** | **测评指标** |
| --- | --- | --- |
| 1 | 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)应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。 |
| 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 |
| 2 | 资产管理 | a)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 |
| b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。 |
| c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理 |
| 3 | 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，实行存储介质专人管理，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 |
| 4 | 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)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效管理，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 |
| c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密 |
| d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 |
| 5 | 漏洞和风险管理 | a) 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。 |
| b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全间题。 |
| 6 | 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 |
| 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 |
| f)应指定专门的部门或人员对H志、监测和报警数据等进行分析、统计，及时发现可疑行为。 |
| g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。 |
| h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。 |
| i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。 |
| j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为 |
| 7 | 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 |
| 8 | b) 应定期验证防范恶意代码攻击的技术措施的有效性。 |
| 9 | 配置管理 | a) 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 |
| b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基 本配置信息库。  |
| 10 | 密码管理 | a) 应遵循密码相关的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 |
| 11 | 变更管理 | a)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。 |
| b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。 |
| c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 |
| 12 | 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。 |
| 13 | 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。 |
| d)对造成系统中断和造成信息泄露的重大安全事件采用不同的处理程序和报告程序。 |
| 14 | 应急预案管理 | a)应规定统 一 的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。 |
| b)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 |
| c)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。 |
| d）应定期对原有的应急预案重新评估，修订完善 |
| 15 | 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。 |
| c)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展 安全运维工作的能力，并将能力要求在签订的协议中明确。 |
| d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感 信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。 |

（四）质量要求：

1.遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果。

2.保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险。

3.对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

4.使用的技术装备、设施应当符合本办法对信息安全产品的要求。

5.供应商应参照《网络安全等级保护基本要求》GB/T 22239-2019标准对被测的信息系统提出建设整改建议和系统整改方案，协助其所有被测系统整改达到等级保护相应级别的标准和要求，出具《信息系统安全等级测评报告》；并对现有被测评的系统进行梳理，协助用户撰写定级报告和备案表、协助到公安部门办理系统备案手续，使系统能够取得公安部门颁发的《信息系统安全等级保护备案证明》。

（五）服务团队要求：

1.供应商应为本项目配备具有丰富经验的测评团队，包含项目经理1名、现场测评人员不少于4名，其中项目经理可由现场测评人员兼任（供应商拟派测评团队人员须是本单位的正式员工，提供人员2025年1月至投标截止之日起任意3个月的社保证明）。

2.项目经理具有3年及以上信息系统等保测评工作经验，具有中级信息安全等级测评师及以上证书（提供项目经理工作年限证明及证书复印件）。

3.现场测评人员具有1年及以上信息系统等保测评工作经验，具有信息安全等级测评师（DJCP）资质或具备高级工程师技术职称（提供现场测评人员工作年限证明及证书复印件）。

## 三、商务要求

| **序号** | **指标项** | **指标要求** |
| --- | --- | --- |
|  | 响应报价 | （1）本项目报价币种为人民币，供应商报价不得超过限价，否则按无效响应处理；（2）供应商的响应报价是指供应商完成本项目要求的全部工作内容的价格体现，包括但不限于服务人员的工资、五险一金、保险、劳保福利、住宿、管理费、加班费等人工成本以及其他成本等合同义务所有款项，不受任何调价因素的影响，在整个履行合同期间有效，采购人不另外支付。 |
|  | 付款方式 | 供应商完成恩施机场网络等级保护测评工作，并取得当地公安机关备案回执，报采购人验收。验收合格，供应商开具合同金额100%的增值税专用发票后，采购人向供应商支付合同金额的100% |
|  | 服务地点 | 恩施机场。 |
|  | 测评期限 | 合同签订后35个日历天内，完成等级保护测评工作，45个日历天内取得当地公安机关备案回执。 |

| **序号** | **指标项** | **指标要求** |
| --- | --- | --- |
|  | 报价 | （1）本项目报价币种为人民币，供应商报价不得超过限价，否则按无效响应处理（2）供应商的报价应包含为完成采购文件提出的设备采购、运输、安装、软件开发、集成、调试、报检以及售后服务等全部相关工作所有可能发生的费用。对在合同实施过程中可能发生的其他费用（如：增加耗材、材料涨价、人工、运输成本增加等因素），采购人概不负责。本文件所要求内容应视为保证设备运行所需最低要求，如有遗漏，供应商应予补充。否则，将不予以付款。 |
|  | 包装和运输 | 货物包装应符合对应货物包装标准规范的相关要求。供应商应选择适当的交通工具对货物进行运输，所交付的货物要有适合长途运输和多次搬运、装卸的坚固包装，运输过程中不得出现箱件破损、设备和零件散失等情况。供应商应按货物特点，按需要分别采取防潮、防霉、防锈、防腐蚀等保护措施，以保证货物在没有任何损坏和腐蚀的情况下安全运抵采购人指定地点。包装、运输及装卸费用由供应商承担。 |
|  | 交货地点 | 恩施许家坪国际机场。 |
|  | 付款方式 |  |
|  | 质量要求 | 符合国家标准和采购人要求。 |
|  | 产品到货验收 | 货物运送至采购人指定地点后，由成交供应商及采购人双方共同对货物进行检验并办理相关移交手续。 |
|  | 售后服务 | 质量保证期内，如采购人发现存在质量问题，采购人仍有权选择要求成交供应商更换或退货。采购人要求更换的，成交供应商应在采购人提出要求后2日内回复意见，并在要求的时间内予以更换；如成交供应商无法更换，或成交供应商未在采购人提出更换要求后2 日内回复，采购人可要求退货。 |
|  | 违约责任 | 如成交供应商未按合同规定时间将产品运到采购人指定地点，每延期一日，成交供应商应向采购人支付总货款千分之二的违约金，延期超过十五日的，采购人亦有权解除该笔采购。 |
|  | 培训 | 成交供应商安排主要设备厂商工程师为采购人相关人员提供安装、操作、一般故障排除等培训，场地、交通等与培训相关的费用均由成交成交供应商承担。 |
|  | 其他要求 | 成交供应商提供的货物未达到采购文件规定要求，且对采购人造成损失的，由成交供应商承担一切责任，并赔偿所造成的损失，其他未尽事宜在合同签订时约定 |
|  | 知识产权 | 采购人无偿享有供应商按照合同提供的货物、软件（如有）、文件资料及所包含知识产权的使用权，且供应商向采购人提供的货物、软件（如有）及相关服务免受第三方提出的侵犯其专利权、商标权、著作权或其他知识产权的主张，任何第三方如果提出此类权利主张，由供应商承担由此产生的费用和后果。 |

## 四、附《湖北机场集团有限公司“供应商不良行为”管理办法》

湖北机场集团“供应商不良行为”管理暂行办法-节选

第一章 总则

本办法所称供应商不良行为，是指正在或有意向为机场集团提供货物、工程、服务或资金的企业、其他经济组织或个人，在与机场集团招标采购（含招商）、签约和履约过程中，违法违规或存在其他不良行为，给机场集团、社会和公众造成损失或不良影响。

供应商不良行为分一般不良行为和严重不良行为。

第二章 不良行为的定义

第四条 供应商“一般不良行为”定义。

（一）采取不正当手段诋毁、排挤其他供应商或故意以虚构事实等方式进行投诉的；

（二）中标（成交）后未按文件规定要求提交履约保证金，给采购方工作造成一定影响的；

（三）中标（成交）后违反投标、竞价承诺或合同约定，擅自提高价格、降低质量标准、无故拖延工期或供货时间，给采购方工作造成影响，情节较轻的；

（四）不能完全履行合同约定，但违约情节较轻的；

（五）其他违背诚实信用原则，情节较轻的行为。

第五条 供应商“严重不良行为”定义。

（一）向集团从事招标采购工作的各类相关工作人员、集团委托的招标代理机构等行贿或者提供其他不正当利益，以及其他可能影响集团相关工作人员公正履行工作职责的；

（二）串通采购人、其他供应商或集团委托的招标代理机构进行投标、围标和竞价，干扰正常招标采购秩序的；

（三）非法以他人名义进行投标、竞价或者以其他方式弄虚作假骗取中标（成交）的；

（四）中标（成交）后，不按照招标文件（采购文件）和中标（成交）供应商的投标文件（响应文件）签订合同，或者要求与采购人另行签订背离合同实质性内容协议的；

（五）合同签订后，无正当理由拒不履行或者拖延履行采购合同义务的，给采购方工作造成影响，情节严重的；

（六）将中标（成交）项目转让（转包）给他人，或者违反招标文件（采购文件）规定，擅自将中标（成交）项目分包给他人的；

（七）擅自变更、中止或终止采购合同，给采购方造成重大经济损失或严重影响生产、建设工期的；

（八）未按合同规定履行合同义务，造成严重的质量问题或给采购方造成严重经济损失、安全事故以及不良社会影响的；

（九）提供虚假材料、虚构事实进行恶意诽谤、诬告、陷害等行为的；

（十）存在其他严重不良行为的。

第三章 不良行为认定

第六条 供应商列入“不良行为”的主要依据：

（一）政府行政主管部门书面认定文件、司法机关的相关生效判决、裁定、决定等；

（二）纪检、监察、审计等部门的调查结果；

（三）项目管理部门、使用单位对供应商合同履约情况的评估或调查；

第四章 不良行为的处罚

第十二条 供应商存在第四条 “一般不良行为”情形之一的，该供应商、该供应商法定代表人（或单位负责人）及其担任法定代表人（或单位负责人）的其他供应商，自列入不良行为之日起2年内不得参与集团招标采购活动。

第十三条 供应商存在第五条 “严重不良行为”情形之一的，该供应商、该供应商法定代表人（或单位负责人）及其担任法定代表人（或单位负责人）的其他供应商，自列入不良行为之日起5年内不得参与集团招标采购活动。

第十五条 供应商对处理决定有异议的，可向集团招标采购部提出申诉。申诉期间，不停止对供应商“不良行为”的处理，但原处理决定被依法停止执行的除外。

第五章 信用修复

第十八条 供应商有下列情形之一的，可进行信用修复：

（一）供应商已履行义务，赔偿损失并消除不良影响，可经原认定程序修复信用；

（二）“不良行为”的限制措施期满后信用自动修复。

第六章 附则

第十九条 本办法由湖北机场集团招标采购部负责解释。

**第四章 询价响应文件格式**

封面：

**询 价 响 应 文 件**

**（正本/副本）**

 **项目名称：**

 **项目编号：**

**（供应商名称）（盖章）**

 年 月 日

**附件一：**

**询价响应书**

（湖北机场集团恩施机场有限责任公司）：

依据贵方 （采购项目名称/项目编号） 项目询价通知书，我方代表（姓名、职务）经正式授权并代表供应商（供应商名称、地址）提交下述文件正本一份，副本 份。

1. 报价一览表；

2、法定代表人身份证明复印件和法定代表人授权委托书；

3、营业执照复印件；

4、供应商基本情况；

5、供应商认为需要提供的有关资料；

在此，我方宣布同意如下：

1. 我方所附《报价一览表》中完全响应询价通知书中采购内容的，报价为（注明币种，并用文字和数字表示报价）。

2. 我方将按询价通知书的约定履行合同责任和义务。

3. 我方已详细审查全部询价通知书，包括（补充文件），对此无异议。

4. 本报价有效期（询价有效期）为自询价之日起共60个日历天。

5. 同意提供按照贵方可能要求的与其报价有关的一切数据或资料。

6. 与本报价有关的一切正式往来信函请寄：

供应商名称（盖章）：

地址： 电子函件：

电话： 传真：

供应商（授权）代表签字：

日期：

开户银行：

帐号/行号：

**附件二：**

**报价一览表**

项目名称：

供应商名称：

|  |  |
| --- | --- |
| 供应商名称 |  |
| 供应商地址 |  |
| 项目名称 |  |
| 总报价（元） |  |
| 服务地点 |  |
| 测评期限 |  |
| 备注 |  |

说明：1.所有价格均系用人民币表示，精确到个数位；

2.此表除保留在响应文件中外，另复制一份签字及加盖公章单独密封装在一个小信封中，作为记录之用。

供应商名称（盖章）：

授权代表签字或盖章：

时间： 年 月 日

**分项报价表**

项目名称：

供应商名称：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **内容**  | **单价** | **数量** | **合计(元)** | **备注** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| ... | ... |  |  |  |  |
| 总价： |  |

注：1、此处所报总价合计金额应与报价一览表中总报价金额一致。

2、投标报价须包含完成本项目全部内容的所有有关费用，包括但不限于供应商的制造、运输、仓储、装卸、培训、管理、利润、应交纳的税费等所有费用，供应商应考虑所有可能存在的风险，谨慎报价。

供应商名称（盖章）：

授权代表签字或盖章：

时间： 年 月 日

**附件三：**

**法定代表人授权书**

（湖北机场集团恩施机场有限责任公司）：

兹授权 同志为我公司参加贵单位组织的（项目名称）询价活动的代表人，全权代表我公司处理在该项目活动中的一切事宜。代理期限从 年 月 日起至 年 月 日止。

授权单位（盖章）：

法定代表人（签字或盖章）：

被授权人（签字）：

签发日期： 年 月 日

附：代理人工作单位：

职务： 性别：

手机号码：

身份证号码：

|  |  |
| --- | --- |
| 粘贴被法定代表人身份证（复印件） | 粘贴被授权人身份证（复印件） |

**附件四：**

**湖北机场集团有限公司“供应商不良行为”管理办法承诺书**

（湖北机场集团恩施机场有限责任公司）：

我单位自愿参与本项目的招标活动，在与湖北机场集团招标采购（含招商）、签约和履约过程中，不存在违法违规且不存在其他不良行为，未给机场集团、社会和公众造成损失或不良影响，并完全遵守《湖北机场集团有限公司“供应商不良行为”管理办法》的规定，现针对《湖北机场集团有限公司“供应商不良行为”管理办法》作如下承诺：

1. 我单位不得采取不正当手段诋毁、排挤其他供应商或故意以虚构事实等方式进行投诉。
2. 不得向集团从事招标采购工作的各类相关工作人员、集团委托的招标代理机构等行贿或者提供其他不正当利益。
3. 不得串通采购人、其他供应商或集团委托的招标代理机构进行投标、围标和竞价，干扰正常招标采购秩序的。
4. 不得非法以他人名义进行投标、竞价或者以其他方式弄虚作假骗取中标（成交）。
5. 中标（成交）后按文件规定要求提交履约保证金。
6. 中标（成交）后完全按照招标文件（采购文件）和投标文件（响应文件）签订合同，不得要求与采购人另行签订背离合同实质性内容协议。
7. 合同签订后，无正当理由不得拒不履行或者拖延履行采购合同义务。
8. 不得将中标（成交）项目转让（转包）给他人，或者违反招标文件（采购文件）规定，擅自将中标（成交）项目分包给他人。
9. 不得擅自变更、中止或终止采购合同。
10. 不得提供虚假材料、虚构事实进行恶意诽谤、诬告、陷害等行为。

供应商（盖章）：

 年 月 日

**附件五：**

**询价文件要求或供应商认为需要提供的其他资料**

# 第五章 采购合同

恩施机场网络安全等级保护测评服务采购

项目服务采购合同

**甲方：湖北机场集团恩施机场有限责任公司**

**乙方：**

**2025年 月 日**

采购方（以下称甲方）：湖北机场集团恩施机场有限责任公司

供货方（以下称乙方）：

乙方为湖北机场集团恩施机场有限责任公司2025年网络安全等级保护测评项目（项目编号：------）服务单位。根据《中华人民共和国政府采购法》、《中华人民共和国民法典》及相关法律法规，双方在平等、互利、友好协商的基础上，本着守法、公平、诚信的原则，就恩施机场信息系统等级保护测评服务相关事宜，经双方协商一致，签订本合同，供双方共同遵守。

**一、工作内容**

对三级系统（安检信息系统）等级保护测评工作以及配合采购人完成相关政府部门的网络安全等级保护相关（测评、登记、备案等）工作要求。

**1.安全测评服务内容**

测评系统范围：

|  |  |  |
| --- | --- | --- |
| **序号** | **设备/系统** | **保护等级** |
| 1 | 安检信息系统 | 三级 |

 具体等级测评要求和输出成果以磋商文件中的要求和乙方响应文件中的要求以孰严为准。

如乙方测评后认为甲方信息系统等级保护测评尚未达到公安部门及相关部门的等级保护检查要求，则乙方应提供安全整改建设方案设计，并指导甲方整改直到达到要求。

**2．安全整改与安全加固**

等级测评完成后，应根据等级测评中发现存在的问题开展安全整改工作，建设信息安全保护设施，建立安全制度，落实安全责任，对信息系统进行保护。

安全加固工作需要有等级测评师或网络与信息安全管理员能力的人员进行加固指导，必要时直接进行加固支持。

**二、甲方责任**

甲方应积极配合乙方进行安全等级测评工作，保证提供的相关资料真实可靠。

因甲方原因或不可抗力使乙方工作延期，经双方友好协商，可顺延工作期限，甲方不承担顺延工期所产生的费用。

因甲方需要变更测评内容而导致乙方工作量或工作时间增加的，乙方应对可能增加的工作量或工作人员等具体情况进行核定并向甲方作出书面说明，甲方对此进行书面确认，但不增加任何费用。甲方发现乙方人员工作不合格，可通知乙方在 3 日内更换，且更换人员和资质不能低于合同要求。

**三、乙方责任**

1. 乙方在合同规定的时间内完成工作，提交工作成果。

2. 因乙方故意或过失导致甲方信息系统被破坏、数据丢失，乙方应及时采取补救措施进行系统和数据的恢复，并根据影响程度承担相应的赔偿责任。

3. 乙方在安全等级测评开展之前，以书面形式通知甲方作好相应的系统数据备份等准备工作，并明示测试方法、采用的测试工具以及可能出现的风险。

4.乙方测评后认为甲方信息系统等级保护测评尚未达到公安部门及相关部门的等级保护检查要求，则乙方应提供安全整改建设方案设计，并指导甲方整改直到达到要求。

5.乙方应遵守与甲方签订之保密协议。乙方应充分保护从甲方直接或间接获取的甲方的商业秘密、技术信息、资料，如无甲方书面同意，乙方不得向任何第三方披露或转让甲方的上述信息。乙方应将甲方提供的资料和/或信息限制在与本次工作有关的人员、保密协议签署的范围内，并妥善保管。若因乙方原因导致甲方资料和/或信息泄漏，乙方依法向甲方承担责任。该条款不因合同的解除、终止而失效。

6.乙方如发现上述资料和/或信息被泄露或者自己过失泄露，应当采取有效措施防止事件进一步扩大，并及时向甲方通报，该条款不因合同的解除、终止而失效。

7.乙方需要在服务期内提供1次网络安全培训。(针对甲方提出的网络安全培训需求，乙方应及时进行响应，在服务期内提供1次网络安全培训工作。培训内容以甲方具体需求为准，包括但不限于网络安全意识培训和网络安全技能培训，培训完后须提供培训小结和考核结果)

8.乙方测评过程中，对整个等保系统进行全面梳理，理清网络结构，出具网络拓扑图，标注设备功能特性及故障后的影响，测评完后对甲方进行系统培训。

9.乙方应该按照本合同约定提供安全巡检服务。

**四、工作成果提交**

1．在安全等级测评工作完毕后，乙方出具书面正式的安全等级测评报告（电子版2份，纸质版3份），并协助甲方获取《信息系统安全等级保护备案证明》（已备案信息系统，如无变更需求，则不再进行备案）。

乙方的安全等级测评报告仅对甲方被测系统测评时的状况负责，不涉及该系统结构或功能等要素发生变化后的情况。

2.其他（如有）：（以磋商文件中的要求和乙方响应文件中的要求以孰严为准）。

**五、服务时间**

在合同签订后 35 个日历天内完成等级保护测评工作，45个日历天内取得当地公安机关备案回执。安全等级测评采用在甲方现场实地进行的方式。乙方在签订合同后 个工作日内对甲方被测系统进行现场考察，除不可抗力或甲方造成的原因外，甲方被测系统通过现场考察后 个工作日内乙方完成安全等级现场测评工作，并向甲方提交不符合项整改方案，在甲方完成整改并提交整改报告之日起 个工作日内完成复测工作，并提交安全等级测评报告。

**六、费用及支付方式**

本合同金额共计人民币（大写）（ 小写：￥ .00 ）元整，该合同价款为固定总价，是乙方提供合同约定全部服务的对价，合同履行过程中，甲方采取以下方式支付合同金额：

乙方在服务期内完成合同约定的所有工作，提交下列文件和单据，并经审核无误30个工作日内之内甲方向乙方支付合同价款的100%：

1）金额为合同价的100%的增值税专用发票；

2）由甲方审核通过的全套测评材料和公安机关颁发的备案证明；

3）由甲方审核通过的全套备案材料；

4）由甲方审核通过的培训小结和考核结果。

乙方延迟提供发票，甲方有权拒绝付款且不承担任何违约责任。未实施内容甲方有权据实扣减。

开票明细：等级保护测评服务甲乙双方账户信息如下：

**甲方：**

户名：湖北机场集团恩施机场有限责任公司

税号：91422800770780066F

单位地址：湖北省恩施市许家坪机场

开户行：中国工商银行恩施分行营业部

账号：1817002409026408523

电话：0718-8410744

**乙方：**

户名：

税号：

单位地址：

开户行：

账号：

电话：

**七、知识产权**

双方约定，乙方出具的安全等级测评报告等成果文件的知识产权由甲方所有。

**八、不可抗力**

1.签约任何一方由于受到诸如战争、严重火灾、洪水、台风、地震、疾病流行、政府行为等不可抗力事件的影响而不能执行合同时，履行合同的期限应予以相应顺延，延长的期限应相当于不可抗力所影响的时间。不可抗力事件系指买卖双方在缔结合同时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事件。

2.受阻一方应在不可抗力事件发生后尽快通知对方，并于事件发生后7天内将有关当局出具的证明文件送交对方审阅确认。一旦不可抗力事件的影响持续30天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

3.如因不可抗力导致合同解除，甲方支付的费用超过乙方工作量的，乙方应据实退还给甲方。

**九、违约金及损失赔偿额的计算**

1．乙方未能按时完成第一条约定的工作内容及第四条约定的工作成果的提交等任何一项工作，每延误一天扣减合同款项的1%，累计延误 90日（含）以上，甲方有权解除合同，乙方应向甲方支付合同价款20%的违约金，并退还甲方已付全部款项。

2．乙方违反本合同第三条及其他条款约定，乙方应赔偿甲方因此所受的损失。

3．除法定及约定条件外，任何一方如单方面提出解除合同的要求，须经对方签字确认并赔偿由此给对方造成的经济损失。

4．其他违约行为按照《民法典》有关规定，由违约方承担违约责任。

5.甲方有权从应付款价款中直接扣除乙方的违约金。

**十、保密条款**

1.甲方应充分保护直接或间接获取的乙方的商业秘密，如技术信息、专有技术、经营信息，无乙方书面同意，甲方不得向任何第三方转让乙方的上述信息。若因甲方原因导致乙方的秘密信息泄漏，甲方依法向乙方承担责任。该条款不因合同的解除而失效。

2.甲方如发现上述资料和信息被泄露或者自己过失泄露，应当采取有效措施防止事件进一步扩大，并及时向乙方通报。该条款不因合同的解除、终止而失效。

3.乙方应遵守与甲方签订之保密协议。乙方应充分保护直接或间接获取的甲方的商业秘密、技术信息、资料，如无甲方书面同意，乙方不得向任何第三方转让甲方的上述信息。乙方应将甲方提供的资料和信息限制在与本次工作有关的人员、保密协议签署的范围内，并妥善保管。若因乙方原因导致甲方资料和信息泄漏，乙方依法向甲方承担责任。该条款不因合同的解除、终止而失效。

4.乙方如发现上述资料和信息被泄露或者自己过失泄露，应当采取有效措施防止事件进一步扩大，并及时向甲方通报，该条款不因合同的解除、终止而失效。

**十一、通知条款**

本合同中任何通知必须采用书面形式。

甲方代表： 乙方代表：

姓名： 姓名：

联系方式： 联系方式：

2.双方确认以上联系方式为本合同约定的联系方式，任何一方的联系方式发生变更的，应当在发生变更后3个工作日内通知对方，否则因此产生的一切不利后果自行承担。

3.双方关于本合同履行及相关事宜的通知、指示、要求、决定等，按照本合同约定的上述联系方式向对方发送。如果以特快专递或挂号信形式寄送的，自发出之日起第3日视为送达之日（无论对方是否拒签或退还）；如果以电子邮件、手机短信形式发送的，自发出起24小时内视为送达（无论对方是否查看邮件或拒收）。

4.上述送达地址作为本合同所涉诉讼文书（包括但不限于传票、判决书、裁定书、调解书、执行裁定书、限期履行通知书等）的有效送达地址。上述送达地址适用于一审、二审、再审和执行等各个诉讼阶段。相关诉讼文书按上述地址进行送达，因无人签收、拒收等原因导致被退回的，退回之日为送达之日。

**十二、争议解决**

1．本合同的未尽事宜，本着安全等级测评顺利实施的原则，由双方友好协商解决。

2. 本合同在履行过程中发生的争议，由甲乙双方友好协商解决，如协商不能达成一致，依法向甲方所在地人民法院起诉。

**十三、其他条款**

1. 本合同连同附件为中文文本，一式陆份，甲方执肆份，乙方执贰份。

2. 本合同自各方法定代表人或授权代表签字并加盖公章或合同专用章生效。

3. 本合同所有的修订、补充和更改都应采用书面形式，并经过双方法定代表人或授权代表签字并加盖公章或合同专用章才能成为合同的一部分。

**附件1：网络信息安全责任书**

**附件2：网络安全等级保护测评项目保密协议**

甲方（盖章）： 乙方（盖章）：

法定代表人（或授权代表）签名： 法定代表人（或授权代表）签名：

日期： 日期：

附件1：网络信息安全责任书

**甲方：湖北机场集团恩施机场有限责任公司**

**乙方：**

为了维护机场网络信息安全，贯彻落实国家《中华人民共和国网络安全法》、现将网络信息安全要求告知乙方，望知悉并遵照执行，并接受甲方监督。

一、乙方人员作业时应按程序要求规范操作，不得安装与工作无关的软件，不得利用机场网络传播非法软件。

二、乙方人员必须注意终端设备的各种账号密码，个人使用的账号密码要定期修改，并具有一定的复杂性（要求长度有8位，包含大小写字母、数字、特殊符号）。禁止将各类生产系统使用权限交与他人使用。

三、涉及生产系统的一切信息，维护人员有义务保持其机密性，不得通过U盘等移动存储设备外泄重要生产资料。

四、乙方人员严禁私自修改IP地址、私自移机、更换电脑硬件等违规操作。

五、不得私自卸载生产终端的防病毒软件、终端准入软件。

六、乙方人员在工作中发现其他人员有违规操作，应立即向甲方监管部门报告，并及时保留证据。

七、因乙方人员违规操作引发的网络信息安全事故，一切责任由乙方公司全部承担。

|  |
| --- |
| 单位（盖章）：法定代表人或授权代表（签字）： 年 月 日 |

附件2：网络安全等级保护测评项目保密协议

甲方：

乙方：

鉴于乙方对甲方的 （项目名称）系统进行网络安全等级测评，为保护甲方的系统秘密，乙方的技术秘密，根据国家法律、法规的有关规定，在友好协商的基础上，双方签订如下保密协议：

**一、保密的内容**

（一）甲方的秘密：包括甲方提供的以及在测评过程中涉及的甲方系统网络拓扑信息、系统配置信息、系统运行的数据、管理制度及流程，以及经甲方声明需要保密的其他信息。

（二）乙方的秘密：包括乙方在此次测评过程中使用的业务流程规范、评估方法、测试方法以及乙方声明需要保密的其他信息。

上述信息必须以如下形式确定其保密性：

对于书面的或其它有形的信息，在交付对方时应标明“专有”或“秘密”字样；

无法标明的信息在透露给对方前应声明是专有信息，进行书面记录。

**二、保密的范围**

（一）乙方只在此次测评需要时才能使用甲方提供的秘密信息。乙方应将甲方提供信息的使用限制在与本次测评有关的人员、保密协议签署者范围内。

（二）甲方应将乙方在此次测评中使用到的业务流程规范、评估方法、测试方法等技术信息限制在与本次测评有关的人员、保密协议签署者范围内。

（三）一方依据法律或政府部门的有效指令而使用对方提供的信息时，应通知对方。

**三、保密义务**

（一）未经许可不得主动获取对方与本次工作无关的秘密信息；

（二）不得向不承担保密义务的任何第三人披露上述秘密信息；

（三）不得协助不承担保密义务的任何第三人使用上述秘密信息；

（四）如无对方预先书面同意，任何一方不得向任何第三方转让上述秘密信息；

（五）如发现上述秘密被泄露或者自己过失泄露，应当采取有效措施防止泄密进一步扩大，并及时向对方报告；

凡未经对方书面同意，一方以直接、间接、书面、口头等形式为第三方提供上述内容的行为均属违反保密义务的行为。

但以下情况不属于违反保密义务：

（一）获取或披露一方已公开发表，或已为公众所知的信息；

（二）获取或披露一方已书面授权公开的信息；

（三）获取的信息属于一方通过合法手段从第三方在未受到任何限制的情况下获得的；

（四）根据法律、法规，司法或行政命令的要求向有关国家机关提供他方的秘密信息。

上述第（四）种情况下必须向资料接受者申明该信息的保密要求，并应当尽最大的努力帮助他方有效地防止或限制该秘密信息的进一步泄露。

**四、保密期限**

甲、乙双方确认，双方的保密义务从本协议签署之日起生效。双方的保密义务期限该条款不因合同的解除、终止而失效。

**五、违约责任**

（一）如果一方不履行本协议第三条所规定的保密义务，应当承担给对方造成的直接损失的赔偿责任。

（二）因一方的违约行为侵犯了另一方的合法权益，另一方可以选择根据本协议要求其承担违约责任，或者根据国家有关法律、法规要求其承担侵权责任。

**六、争议的解决**

甲乙双方友好协商解决本协议中的争议。协商不成的，任何一方都有权向甲方所在地法院提起诉讼。

|  |  |
| --- | --- |
| 甲方（盖章）：法定代表人或授权代表签名：联系电话：日期： 年 月 日 | 乙方（盖章）：法定代表人或授权代表签名：联系电话： 日期： 年 月 日 |

**七、协议的效力和变更**

本协议的任何修改必须经过双方的书面同意