项目比价文件

 枝江市人民医院就网络安全等级保护测评项目进行比价采购，现邀请你公司前来参与报价。

1. 项目编号:
2. 项目名称: 枝江市人民医院网络安全等级保护测评
3. 采购内容：

 枝江市人民医院网络安全等级保护测评

A 服务采购

**（一）采购内容及说明**

明确被测系统的安全等级是开展信息系统安全等级保护测评工作的首要步骤，依据《信息安全技术网络安全等级保护定级指南》GB/T 22240-2021,结合科学的方法、规范的流程以及系统业务特性，实现对信息系统的安全定级。

信息系统定级服务主要包括：信息系统调查、定级对象分析、定级要素分析、撰写定级报告和协助定级备案五个组件。

根据定级指南要求，按上述步骤，协助采购方完成被测信息系统定级、指导采购方编写定级、备案材料，配合采购方到宜昌市公安局办理系统定级、备案手续，确保信息系统安全保护等级定级准确、备案完整。确保采购人达到信息安全等级保护达到三级，并取得《信息安全等级保护备案证明》，特别是必须包括医院集成平台软件系统。

**（二）采购需求一览表(列明货物名称、规格型号、采购数量及单位)。**

| **序号** | **名称** | **达到目的** |
| --- | --- | --- |
| 1 | 定级、备案服务 | 对枝江市人民医院指定的信息系统进行梳理，了解信息系统的基本情况，撰写定级报告、填写备案材料，协助采购方到宜昌市公安局办理信息系统的定级、备案证明。 |
| 2 | 测评报告 | 依据《网络安全等级保护测评报告模版》，出具符合格式要求的《网络安全等级保护测评报告》提交给采购方。 |
| 3 | 编制信息安全管理制度 | 对现有的管理制度进行梳理，依据GB/T 22080-2016《信息安全技术 信息安全管理体系要求》，由高级工程师协助实施，完善现有的管理制度体系，具体内容包括：总体安全规划、机房安全、安全管理规范、组织架构、岗位设置、人员管理、应急响应和演练、安全培训、信息安全策略等管理制度体系的建设。 |
| 4 | 安全建设整改方案 | 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 22080-2016信息技术 安全技术 信息安全管理体系要求》、《GB/T 22081-2016信息技术 安全技术 信息安全管理实用规则》等标准规范的第三级要求，对被测评系统提出整体的安全建设整改方案，协助采购方进行安全整改，确保使用的网络、边界安全、主机应用和数据库等相关安全产品能够满足等级保护标准基本要求，使被测系统达到相应级别的安全防护能力。 |

**(三）参数要求**

**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 |
|  | 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。 |
| 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 温湿度控制 | a) 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。 |
| c) 应设置冗余或并行的电力电缆线路为计算机系统供电。 |
|  | 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、关键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、重要配置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 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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 |
|  | 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**

测评对象主要为：应用系统、操作系统、数据库、中间件、终端等。涉及工作单元11个，具体如下表：

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 测评指标 |
|  | 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。 |
|  | 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。 |
|  | 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 |
|  | 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。 |
|  | 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 |
|  | 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 | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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**

测评对象主要为：提供集中系统管理功能的系统、数据库审计系统、综合安全审计系统。涉及工作单元4个，具体如下表：

|  |  |  |
| --- | --- | --- |
| 序号 | 工作单元名称 | 测评指标 |
|  | 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。 |
|  | 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 | 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。 |
|  | 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 |
|  | 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。  |
| 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。  |
|  | 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 |
|  | 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。 |
|  | 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。 |
|  | 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。  |
|  | 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 | 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 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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同家有关规定。 |
|  | 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 |
|  | 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做出规定。 |
| 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质文档和移动介质等。 |
|  | 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做出规定，并对信息的使用、传输和存储等进行规范化管理。 |
|  | 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。 |
|  | 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。 |
|  | 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问题。  |
|  | 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日志、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。 |
|  | 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) 应定期验证防范恶意代码攻击的技术措施的有效性。  |
|  | 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。  |
|  | 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。 |
|  | 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。 |
|  | 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。 |
| 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。 |
|  | 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。 |
|  | 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）商务要求：

1、工期：合同签订后的3个月内完成，并取得《信息安全等级保护备案证明》，达到三级标准，但因采购人整改耽误的时间不计算在内。

2、付款方式：采购人取得《信息安全等级保护备案证明》时支付合同款的90%，余款一年后一次性付清。

3.交货地点:枝江市人民医院

四、采购预算:6万元

五、供应商资格条件**（所有资料需加盖公章，不按要求提供资料为废标）：**

1、提供合法有效的企业法人营业执照复印件。

2、提供法人授权委托书，法人和委托代理人身份证复印件附后。投标人与法人身份一致的，提供法定代表人资格证明文件，法人身份证复印件附后**（递交响应文件时需另外提供一份用于审查投标人身份，与密封的投标文件单独分开提供）**。

3、投标报价表。

4、提供“信用中国” 网站或者中国政府采购网等渠道查询的主体信用记录，未被列入信用记录失信被执行人、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的网站截图加盖公章。

5、提供国家公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》的复印件并加盖公章。省外等级保护测评机构须提供在湖北省网络安全等级保护工作领导小组办公室办理异地测评备案手续的相应证明文件。

6、供应商需具有专业化的项目实施队伍或具备公安机关认可的攻防演练实验室或具有“院士专家工作站”；项目实施负责人应具有等级保护高级测评师或高级工程师资质；项目实施人员必须具有等级测评师资质（DJCP），等级测评师不少于5人。（提供相应证明文件复印件加盖公章）。

6、投标人认为需要提供的其他资料。

7、投标人应当编制响应文件正本一份，**必须进行胶装**。响应文件不得行间插字、涂改或增删。如有修改错漏处，必须由响应文件签署人签字或盖章，否则视为无效文件。上述投标资料需装入档案袋，密封盖章。

注：投标人应仔细阅读招标文件的所有内容，按要求提供完整的投标文件，并保证全部资料的真实性，以使其投标对招标文件做出实质性响应，否则其投标可能被拒绝,责任由投标方承担。

六、优惠政策：对小微企业报价给予6%-10%的价格扣除，用扣除后的价格作为评审价进行价格排序。（采购人根据实际情况自行确定价格扣除比例）。

七、获取比价文件和报名

1.发放时间：2022年5月 日起至2022年5月 日止（上午：8:30-12:00，下午14:00-17:30）。

2.发放方式： 网上下载 。

3.发放地点：三峡枝江网http://www.zhijiang.gov.cn/)免费领取。

八、响应文件编制

1.供应商应认真阅读、并充分理解本比价文件的全部内容（包括所有的补充、修改内容），承诺并履行本比价文件中各项条款规定及要求。

2.响应文件应按本文件的全部内容，包括所有的补充通知及附件进行编制。

3.如因供应商只填写和提供了本文件要求的部分内容和附件，比价小组将拒绝其补充。

4.响应文件的组成

不限于以下内容，如未提供，比价小组有权拒绝其响应文件：

**A 货物服务类采购项目**

（1）报价一览表；

（2）分项报价表；

（3）货物及服务清单；

（4）技术和服务响应、偏离情况说明表；

（5）法人（负责人）代表授权书；

（6）本比价文件“五、供应商资格条件”所列要求的相关证明材料；

（7）《中小企业声明函》（如果有）；

（8）本比价文件要求提供的其他文件及资料。

九、响应文件份数及封装

供应商只需提交一份响应文件，响应文件密封包装在一个包装袋内，并在包封上注明供应商名称和采购项目名称。封包袋封口上加盖公司公章，并注明“比价时间以前不得开封”字样。

十、响应文件递交

1.截止时间：2022年5月 日15时0分

2.地点：请将纸质版响应文件密封递交至湖北省枝江市友谊大道61号枝江市人民医院小会议室，响应文件递交截止时间即为比价时间，逾期送达的响应文件概不接受。

## 3.投标人必须提供48小时内核酸检测阴性报告，否则不能参与投标。

十一、评审方法

1.响应文件审查。采购人确定3人以上单数比价小组，比价小组根据本比价文件规定的供应商资格条件、评定成交的标准等事项对供应商提交的响应文件进行资格性和符合性评审。

资格性审查和符合性审查内容及标准

|  |  |  |
| --- | --- | --- |
| 序号 | 检查内容 | 检查标准 |
| 1 | 资格性检查 | 具有独立承担民事责任的能力 | 提供合法有效的营业执照或事业单位法人证书复印件，加盖公章。 |
| 信用记录 | 响应文件递交截止时间当天，在“信用中国”网站(www.cred itchina.go v.cn)、中国政府采购网(www.cc gp.gov.cn) 查询，供应商未被列入信用记录失信被执行人、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，以现场查询的为准。 |
| …… |  |
| 2 | 符合性检查 | 供应商名称 | 供应商名称是否与营业执照一致。 |
| 响应文件签署 | 按比价文件要求在规定区域加盖单位章，法定代表人或授权代表签字。 |
| 法定代表人和授权代表资格 | 具有法定代表人资格证明和法定代表人授权委托书。 |
| 报价是否有效 | 只有一个有效报价且未超过采购预算价。 |
| 货物或者服务清单 | 满足本比价文件“三、采购内容”要求。 |
| 交货期、质量要求 | 满足本比价文件“三、采购内容”要求。 |
| 其他要求 | 符合法律法规和本比价文件规定的其他实质性要求。 |
|  |  | …… |  |

说明：采购人应根据项目类别和实际情况可对上表中的资格性审查和符合性审查的内容进行修改。资格性和符合性审查不合格，技术、商务及服务不满足本比价文件要求的，响应文件按无效文件处理。

评审后，满足本比价文件要求的供应商不足3家的，采购活动终止，采购人重新组织采购。满足本比价文件要求的供应商达到3家以上，比价小组对满足要求的供应商进行价格评议。

2.价格评议。比价小组根据本比价文件“六、优惠政策”相关规定，结合供应商提供的《中小企业声明函》，对供应商报价进行价格扣除评议，用扣除后的价格作为评审价进行价格排序，评审价不作为合同价格，合同价格应为供应商实际报价。供应商提供本企业制造的产品、承担的工程或者服务的，应由供应商出具《中小企业声明函》，供应商提供其他小型和微型企业制造的产品的，应由产品制造企业出具《中小企业声明函》原件，否则，不给予价格扣除。

3.推荐供应商。比价小组从满足本比价文件实质性要求的供应商中，按照评审价由低到高的顺序提出3名以上成交候选供应商，并编写评审报告。

十二、确定成交供应商

1.比价小组应当在评审结束后1个工作日内将评审报告送采购人，采购人应当在收到评审报告后1个工作日内，从比价小组推荐的候选供应商中，根据满足比价文件要求且评审价最低的原则确定成交供应商。

2.确定成交供应商后，采购人应将成交结果在三峡枝江网或枝江市公共资源交易信息网等网络媒体予以公示，同时向成交供应商发出成交通知书。

十三、签订采购合同

成交供应商收到成交通知书后，应在3个工作日内与采购人签订采购合同。

十四、联系方式：

联 系 人：魏丹

联系电话：18871742296

地 址：湖北省枝江市友谊大道61号

 采购人（公章）

 年 月 日

 附

响应文件格式

项目

响 应 文 件

项目编号：（如有）

 项目名称：

 供应商名称（盖章）：

 日 期： 年 月 日

响应文件组成（货物服务类）

目 录

（1）报价一览表；

（2）分项报价表；

（3）货物及服务清单；

（4）技术和服务响应、偏离情况说明表；

（5）法人（负责人）代表授权书；

（6）本邀请函“五、供应商资格条件”所列要求的相关证明材料；

（7）《中小企业声明函》（如果有）；

（8）本邀请函要求提供的其他文件及资料。

报价一览表

项目编号:（如有）

项目名称:

|  |  |
| --- | --- |
| 总报价 | 大写：小写： |
| 其他 |  |

供应商名称（公章）：

授权代表（签字）:

日 期：年 月 日

报价组成情况表

项目编号：（如有）

项目名称：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称（服务） | 规格型号 | 制造商名称 | 单位 | 数量 | 单价 | 总价 |
| 1 |  |  |  |  |  |  |  |
| 2 | … |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 | … |  |  |  |  |  |  |
| 6 | 其它 |  |  |  |  |  |  |
| 总计 |  |

说明：1.所有价格均用人民币表示，单位为元。

 2.分项报价总计价格必须与《报价一览表》报价一致。

供应商名称（公章）：

授权代表（签字）:

时间：年 月 日

货物、服务清单

项目编号：（如有）

项目名称：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物/服务名称 | 主要规格、技术参数 | 数 量 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| … |  |  |  |

说明：按技术参数要求，提供所投货物详细的技术规格、参数及要求。

供应商名称（签章）：

供应商法定代表人（签章）：

日期：年 月 日

技术和商务条款响应、偏离说明表

项目编号：（如有）

项目名称：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 邀请函要求 | 响应文件具体响应内容 | 响应/偏离 | 说明 | 响应文件中对应的页码 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| … |  |  |  |  |  |

注：1.供应商须对照邀请函“ 三、采购内容”要求，进行逐条说明是否满足要求，并申明与技术规格条款的响应和偏离。

2.技术参数中带“★”参数要求必须满足，均不得负偏离，否则为无效响应。

法人代表授权书

（采购人名称）：

兹授权 同志为我单位参加贵单位组织的编号为（项目编号）的（项 目 名 称）采购活动的代表人，全权代表我单位处理在该项目采购活动中的一切事宜。代理期限从年月日起至年月日止。

供应商名称（签章）：

签发日期：年 月 日

附：

代理人工作单位：

联系电话（手机）：

身份证号码：

|  |
| --- |
| 粘贴被授权人身份证（扫描件） |

制造商中小企业声明函

（适用于货物类项目）

（采购人名称）：

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准（详见《中小企业划型标准》），本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。

2.本公司授权 （供应商） 参加（采购人）的 项目（项目编号：\_\_\_\_\_）采购活动提供本企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

3.由本公司制造的货物清单见下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 品牌规格型号 | 数量 | 单价(元) | 分项合计(元) | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
| 合计 |  |

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

说明：1、供应商所投货物为自己制造的，也应按本声明函格式填写。

 2、组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

 3、以联合体方式参与项目投标的供应商，则应由联合体双方签字盖章。

制造商（公章）：

制造商法定代表人（签字或盖章）：

日期： 年 月 日

中小企业声明函

（适用于服务类项目）

（采购人名称）：

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准（详见《中小企业划型标准》），本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。

2.本公司参加（采购人）的 项目（项目编号：\_\_\_\_\_\_）采购活动由本企业承担工程（或提供服务）。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

说明：1.组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

2.以联合体方式参与项目投标的供应商，应由联合体双方签字盖章。

供应商（公章）：

供应商授权代表（签字）：

日期：年 月 日

响应文件组成（工程类）

目 录

（1）报价一览表；

（2）法人（负责人）代表授权书；

（3）项目组人员配备情况；

（4）项目负责人简历表；

（5）项目技术负责人简历表；

（6）中小企业声明函；

（7）价格文件；

（8）技术文件；

（9）本邀请函要求提供的其他文件及资料。

报价一览表

项目编号:（如有）

项目名称:

|  |  |
| --- | --- |
| 总报价（元） |  |
| 工期（天） |  |
| 项目负责人 |  |

注：所有价格均用人民币表示，单位为元。

供应商名称（签章）：

供应商法定代表人（签章）：

日期：年 月 日

法人代表授权书

（采购人名称）：

 兹授权 同志为我单位参加贵单位组织的编号为（项目编号）的（项 目 名 称）采购活动的代表人，全权代表我单位处理在该项目采购活动中的一切事宜。代理期限从年月日起至年月日止。

供应商名称（签章）：

签发日期：年 月 日

附：

代理人工作单位：

联系电话（手机）：

身份证号码：

|  |
| --- |
| 粘贴被授权人身份证（扫描件） |

项目组人员配备情况表

项目编号:（如有）

项目名称:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 职务 | 姓名 | 职称 | 执业或职业资格证明 | 已承担在建工程情况 |
| 证书名称 | 级别 | 证号 | 专业 | 项目数 | 主要项目名 称 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 一旦我单位成交，将实行项目经理负责制，并配备上述项目管理机构。我方保证上述填报内容真实，若不真实，愿按有关规定接受处理。项目管理班子机构设置、职责分工等情况另附资料说明。 |

说明：要求持证上岗的专业技术人员需提供资格证书清晰扫描件。

项目负责人简历表

项目编号:（如有）

项目名称:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 |  | 性别 |  | 年龄 |  |
| 职务 |  | 职称 |  | 学历 |  |
| 参加工作时间 |  | 担任项目经理年限 |  |
| 在建和已完工程项目 |
| 建设单位 | 项目名称 | 建设规模 | 开、竣工日期 | 在建或已完 | 工程质量 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

 注：表后应附有关证明材料。

项目技术负责人简历表

项目编号:（如有）

项目名称:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 |  | 性别 |  | 年龄 |  |
| 职务 |  | 职称 |  | 学历 |  |
| 参加工作时间 |  | 担任项目经理年限 |  |
| 在建和已完工程项目 |
| 建设单位 | 项目名称 | 建设规模 | 开、竣工日期期 | 在建或已完 | 工程质量 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

说明：表后应附有关证明材料。

中小企业声明函

（适用于工程类项目）

（采购人名称）：

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准（详见《中小企业划型标准》），本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。

2.本公司参加（采购人）的 项目（项目编号：\_\_\_\_\_\_）采购活动由本企业承担工程（或提供服务）。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

说明：1.组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

2.以联合体方式参与项目投标的供应商，应由联合体双方签字盖章。

供应商（公章）：

供应商授权代表（签字）：

 日 期：年 月 日