采购编号：N5105032024000002

# 区人医网络安全设备升级采购项目

# 采购需求

泸州市纳溪区人民医院

四川国际招标有限责任公司

共同编制

2024 年 1 月

**一、招标项目简介：**

1.本项目1个包，拟采购服务供应商1名，为泸州市纳溪区人民医院提供网络安全设备升级1批。清单如下：

| 品目号 | 标的名称 | 单位 | 数量 | 单价最高限价（人民币元） | 是否允许购买进口产品 | 是否为核心产品 | 预算金额（最高限价）（人民币元） | 质保期 |
|---|---|---|---|---|---|---|---|---|
| 01-01 | 数据库审计 | 套 | 1 | 50000 | 否 | 否 | 400000 | 合同签订之日起3年内硬件软件均验收合格 |
| 01-02 | VPN | 套 | 1 | 10000 | 否 | 否 | | |
| 01-03 | 堡垒机 | 套 | 1 | 50000 | 否 | 否 | | |
| 01-04 | 漏洞扫描 | 套 | 1 | 26000 | 否 | 否 | | |
| 01-05 | 网闸 | 套 | 1 | 15000 | 否 | 否 | | |
| 01-06 | WAF | 套 | 1 | 70000 | 否 | 否 | | |
| 01-07 | 入侵防御 | 套 | 1 | 29000 | 否 | 否 | | |
| 01-08 | 日志审计 | 套 | 1 | 50000 | 否 | 否 | | |
| 01-09 | 杀毒软件 | 点 | 100 | 400 | 否 | 否 | | |
| 01-10 | 防火墙 | 台 | 1 | 30000 | 否 | 是 | | |
| 01-11 | 上网行为管理 | 台 | 1 | 30000 | 否 | 否 | | |

2.本项目所属行业

| 品目号 | 标的名称 | 标的所属行业 | 是否属于优先采购节能产品 | 是否属于强制采购节能产品 | 是否属于优先采购环境标志产品 |
|---|---|---|---|---|---|
| 01-01 | 数据库审计 | 工业 | 否 | 否 | 否 |
| 01-02 | VPN | 工业 | 否 | 否 | 否 |
| 01-03 | 堡垒机 | 工业 | 否 | 否 | 否 |
| 01-04 | 漏洞扫描 | 工业 | 否 | 否 | 否 |
| 01-05 | 网闸 | 工业 | 否 | 否 | 否 |
| 01-06 | WAF | 工业 | 否 | 否 | 否 |
| 01-07 | 入侵防御 | 工业 | 否 | 否 | 否 |
| 01-08 | 日志审计 | 工业 | 否 | 否 | 否 |
| 01-09 | 杀毒软件 | 工业 | 否 | 否 | 否 |
| 01-10 | 防火墙 | 工业 | 否 | 否 | 否 |
| 01-11 | 上网行为管理 | 工业 | 否 | 否 | 否 |

注：1.“所属行业”即标的所属行业，包括：①农、林、牧、渔业；②工业（包

括采矿业，制造业，电力、热力、燃气及水生产和供应业）；③建筑业；④批发业；⑤零售业；⑥交通运输业（不含铁路运输业）；⑦仓储业；⑧邮政业；⑨住宿业；⑩餐饮业；⑪信息传输业（包括电信、互联网和相关服务）；⑫软件和信息技术服务业；⑬房地产开发经营；⑭物业管理；⑮租赁和商务服务业；⑯其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）以上行业分类详见《国民经济行业分类》(GB/T 4754—2017）及《2017 国民经济行业分类注释》。

3.本项目不专门面向中小企业采购。

## 二、商务要求

1.实施时间：自合同签订之日起 30 日历天内完成验收。

2.实施地点：泸州市纳溪区人民医院。

3.付款方法和条件：

3.1 合同签订后，成交供应商按照合同约定及要求供货、安装、调试完成，并经双方共同验收合格后支付合同总金额的 40%。验收合格之日起：一年内支付合同总金额的 55%；一年后供应商未出现任何违约情况，达到付款条件 30 日内支付合同剩余金额 5%。

3.2 采购人支付费用前，成交供应商向采购人提供正规的发票。

4.质保期要求：全部通过验收后，成交供应商须提供不少于 3 年的软硬件技术维保。

5.供应商所提供的维保、升级服务，需与现网运行安全系统完全兼容，保证安全系统运行与安全功能生效的连续性。

6.投标报价：本项目报价为总价包干合同（交钥匙工程），投标报价包含供应商完成本项目的所有费用，包括产品成本、人员差旅、保险、安装、调试，培训，售后（含质保期内升级和软硬维保）、税金、风险、管理等所有费用；采购人在质保期结束前不再支付其他任何费用。

7.安全保密性：成交供应商与采购方签订保密协议，成交供应商在实施服务过程中获取的任何相关医院信息及病患信息均须保密，未经采购人同意严禁泄露给第三方，如因成交供应商过失导致的信息泄露引发的纠纷及社会不良影响，由成交供应商承担相关法律及经济赔偿责任。

8.日常维护要求：

1）质保期内费用已经包含在投标报价中，不再收取费用；

日常维护：提供 7×24 小时服务；8 小时工作时间内，10 分钟电话响应，对于电话、远程均不能解决问题的 60 分钟到场维护；8 小时工作时间外，20 分钟电话响应，对于电话、远程均不能解决问题的 2 小时到场维护。

9.验收要求：

9.1 履约验收主体：采购人。

9.2 履约验收时间：供应商提出验收申请之日起 30 日内组织验收。

9.3 验收组织方式：自行验收。

9.4 履约验收程序：一次性验收。

9.5 技术履约验收内容：按照本项目采购文件中“技术、服务要求”及成交供应商响应文件进行验收。

9.6 商务履约验收内容：按照本项目采购文件中“商务要求”及成交供应商响应

文件进行验收。

9.7 履约验收标准：验收严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）的要求组织验收，以采购文件、合同要求及成交供应商响应文件技术响应为准。如出现未在采购文件中明确规定的，以行业相关标准为准。如采购双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在采购与成交供应商的响应文件中按质量要求和技术指标、行业标准比较优胜的原则确定该项的约定标准进行验收。

9.8 验收程序和内容：商务条款和技术条款均逐条验收。

9.9 验收相关事宜及法律责任：如出现成交供应商提供虚假材料谋取成交或达不到采购要求的，采购方有权按政府采购相关法律法规向采购方同级财政部门汇报，追究其相关法律责任。

9.10 风险处置措施和替代方案：

9.10.1 风险处置措施：除不可抗力或者合同履行将损害国家利益和社会公共利益导致合同无法履行或者履行没有意义外，成交供应商不得放弃成交，供应商无故放弃成交的将承担以下风险 1.通报同级财政部门。

9.10.2 替代方案：本项目无替代方案。

10.知识产权

10.1 供应商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，由供应商承担所有相关责任。

10.2 如采用供应商所不拥有的知识产权，则在投标报价中必须包括合法获取该知识产权的相关费用。

11.违约责任与解决争议的方法：

11.1 采购双方均应遵守合同约定，非因不可抗力而单方面终止执行合同的，将赔偿因违约给对方造成的经济损失，并向对方支付合同总额 10%的违约金，如因成交供应商原因造成的，采购人除了不予退还履约保证金（如涉及）外，采购人还将提请项目同级财政部门将其列入不良行为记录。

11.2 若因成交供应商原因在合同规定期限内无法交货，采购人有权终止合同，采购人不予退还履约保证金（如涉及）并由成交供应商向采购人支付合同总额 10%的违约金；或经采购双方协商同意继续履行合同，采购人不予退还履约保证金（如涉及），采购人视情况在延迟交货期内每天按合同总额 3‰的标准收取违约金。因不可抗拒力所导致的交货及付款延迟等按照《中华人民共和国民法典》有关条文处理。

11.3 成交供应商交付的货物质量不符合合同规定的，成交供应商应向采购人支付合同总价的 5%的违约金，并须在合同规定的交货时间内更换合格的货物给采购人，否则，视作成交供应商不能交付货物而违约，按合同相关约定进行处理。采购人可将成交供应商货物交给具有法定资格条件的质量技术监督机构检测。

11.4 成交供应商保证本合同货物的权利无瑕疵，包括货物所有权及知识产权等权利无瑕疵。如任何第三方经法院（或仲裁机构）裁决有权对上述货物主张权利或国家机关依法对货物进行没收查处的，成交供应商除应向采购人返还已收款项外，还应另按合同总价的 10%向采购人支付违约金并赔偿因此给采购人造成的一切损失。

11.5 成交供应商应严格遵守服务承诺，如有违约，将赔偿因服务违约给采购人

造成的经济损失。若因成交供应商未按承诺的响应及到场维修时间进行排除故障，采购人有权部分或全部扣除履约保证金（如涉及）；若采购人电话通知成交供应商，未按承诺时限到场维修，超过1天未解决问题的，采购人将追究成交供应商服务违约的相关责任。

11.6 采购人由于不可抗力的原因不能履行合同时，应及时向成交供应商和项目同级财政部门通报不能履行或不能完全履行的理由；成交供应商由于不可抗力的原因不能履行合同时，应在交货时间到期以前及时向采购人和项目同级财政部门通报不能履行或不能完全履行的理由；在取得有关主管机关证明以后，可以签订延期履行、部分履行补充合同或者不履行合同，并根据情况可部分或全部免予承担违约责任。

11.7 解决争议的方法：合同履行期间，若双方发生争议，双方本着友好合作的态度，对合同履行过程中发生的违约行为进行及时的协商解决或由有关部门调解解决，如不能协商解决可向合同签约地法院通过法律诉讼解决。

12 成交供应商在履约期间所产生的劳务纠纷和意外事故等均由成交供应商自行承担。【在响应文件单独提供承诺函】

**注：以上商务条款为实质性条款，均不允许负偏离，负偏离视为非实质性响应投标文件，做无效投标处理，所有商务条款须按采购文件要求在商务响应表中予以应答。**

## ★三、技术、服务要求

| 品目号 | 产品名称 | 技术参数要求 | 单位 | 数量 |
|---|---|---|---|---|
| 01-01 | 数据库审计 | 1.提供数据库审计≥3年正版软件相关序列号，能确保采购人现有设备奇安信DAS1000-TF10-UP-1Y的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |
| 01-02 | VPN | 1.提供VPN≥3年正版软件相关序列号，能确保采购人现有设备奇安信网神X1500-TY14-1Y的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |

| | | | | |
|---|---|---|---|---|
| 01-03 | 堡垒机 | 1.提供堡垒机≥3 年正版软件相关序列号，能确保采购人现有设备奇安信网神 C6100-BH-TF10-PWS 的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |
| 01-04 | 漏洞扫描 | 1.提供漏洞扫描≥3 正版软件相关序列号，能确保采购人现有设备奇安信网神 S1500-TZSJ010P 的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |
| 01-05 | 网闸 | 1.提供网闸≥3 年正版软件相关序列号，能确保采购人现有设备奇安信网神 G1500-TY10P-SWB 的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |
| 01-06 | WAF | 1.提供 Web 应用防火墙≥3 年正版软件相关序列号，能确保采购人现有设备奇安信网神 W1500-VD-M01 的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |
| 01-07 | 入侵防御 | 1.提供入侵防御≥3 年正版软件相关序列号，能确保采购人现有设备奇安信网神 P3000-IPS-01 的合法正常使用。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |

| | | | | |
|---|---|---|---|---|
| 01-08 | 日志审计 | 1.软硬件一体化设备,标准1U机箱，事件综合处理性能≥2000EPS,≥6个千兆电口，≥2T硬盘,≥30授权节点。提供≥3年软硬件维保服务。<br>2.支持对IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。<br>3.支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。<br>4.支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。<br>5.支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化；<br>6.支持机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成。<br>7.日志解析字段内置≥130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等6种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。<br>8.支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息。<br>9.为实现对流量和日志分析的精细化检测和控制，需支持语境关联分析功能（提供支持语境关联分析功能类的软件著作权证书复印件）。<br>10.系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；<br>11.系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告（提供相关功能截图证明材料）<br>12.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 套 | 1 |

| | | | | |
|---|---|---|---|---|
| 01-09 | 杀毒软件 | 1. 提供防病毒（不含第三方扩展引擎）、补丁管理、主机防火墙、终端管控功能≥3 年正版软件相关序列号。<br>2.符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | 点 | 100 |
| 01-10 | 防火墙 | 1、1U 机箱，单电源，至少配置 6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽，另有≥1 个扩展板卡插槽，≥1 个 Console 口，≥64G 固态硬盘存储。推荐开启基础功能最大适用带宽≥500M，单独开启 IPS 功能最大适用带宽≥350M，单独开启防病毒最大适用带宽≥350M，高级功能全开启最大适用带宽≥250M;<br>2、提供≥3 年应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务;提供≥3 年硬件维保、软件升级服务及远程技术支持服务(400 电话支持、Email 支持)。<br>3、支持与现网运行的终端安全管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。<br>4、支持配置基于 IPv6 地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL 过滤、应用识别、反间谍软件等安全功能。<br>5、支持虚拟防火墙功能，在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计。<br>6、支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供相关功能截图证明材料）。<br>7、支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果。<br>8、产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息。<br>9、支持基于主机或威胁情报视图，统计网络中 | 台 | 1 |

| | | | | |
|---|---|---|---|---|
| | | 确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。<br>10、支持接收针对突发重大安全事件的“应急响应消息”，在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果。<br>11、符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | | |
| 01-11 | 上网行为管理 | 1、标准 1U 机箱，至少配置 4 个 10/100/1000M 自适应电口(其中含 1 个管理接口和 1 个 HA 接口)，支持≥1 个扩展插槽，≥128G 固态硬盘，单交流电源。建议 60M 带宽以下网络环境使用;最大并发连接数为 30 万，最大新建连接数为 1.5 万/秒;<br>2、提供≥3 年软件版本与协议库 升级服务;提供≥3 年的 Web 安全防护服务使用授权(含杀毒，恶意 URL 防护，威胁情报订阅服务);主机≥3 年硬件维保及远程技术支持服务(400 电话支持、Email 支持)。<br>3、提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。<br>4、支持自动识别网络中终端的 IP 地址、MAC 地址、终端类型、操作系统、终端厂商和网卡厂商等信息；支持自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别，至少识别≥10 种移动终端型号；对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及厂商、系统、端口等详细信息。<br>5、支持对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制；为覆盖工作无关应用，移动应用≥5000 种，即时消息应≥200 种，虚拟货币交易平台≥40 种；为规避外发类风险，论坛发帖应不低于 3000 种，代理隧道≥100 种；应用协议库包含的应用数量≥12000 种，应用规则总数≥73000 种。<br>6、支持基于文件后缀的文件类型识别；支持基于文件内容对归档文件、压缩文件、加密文件、脚本文件等≥170+文件类型识别。修改后缀名，压缩等方式均可以识别准确类型，支持解析 | 台 | 1 |

| | | | | |
|---|---|---|---|---|
| | | office 系列、pdf、wps 类型文件的内容识别；支持 tar、zip、rar 等≥29 种压缩文件解压缩，支持最大 10 层文件解压缩。<br>7、支持针对 QQ 账号制定策略，对聊天、登录及登出的行为进行记录与控制，对 QQ 文件传输行为、QQ 聊天内容进行审计；支持对微信 windows 版客户端进行聊天内容、外发文件进行内容审计，支持记录发送/接受信息的微信账号，支持记录钉钉聊天行为和内容，记录传输文件。<br>8、可审计、控制 Oracle,MySql,SqlServer, PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等（提供相关功能截图证明材料）。<br>9、支持对域名服务器、数据库服务器、文件服务器、邮件服务器、Web 服务器等业务系统进行传输行为监测，能够及时中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为；支持对上传到业务系统的文件进行病毒查杀，支持本地查杀及病毒文件 MD5 云查。<br>10、支持本地、LDAP、LDAPS、Radius、邮件认证、钉钉、企业微信、蓝信，CAS、OAuth 认证、动态口令 ID 联动的动态二维码认证方式的 WEB 认证。支持在界面上通过配置，将一台设备作为独立的认证服务器配合审计设备使用，提升认证性能；支持终端用户账号绑定手机号码、微信号，绑定后可以通过手机验证码或微信扫码实现上网快捷登录认证，提高用网便捷性。<br>11、支持业务系统访问及 API 接口进行双向扫描、通过敏感信息、安全漏洞、行为接口、自定义接口规则等识别并标识数据及传输风险；对业务访问和 API 接口请求进行内容详情记录，支持列表视图查看记录日志。（提供相关功能截图证明材料）<br>12、符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求（提供由具备资格的机构安全认证合格或安全检测符合要求的证明材料）或提供在有效期内的《计算机信息系统安全专用产品销售许可证》。【提供证明材料或证书复印件】 | | |

注：

1.以上技术服务要求（所有条款均为“★”条款）均为实质性要求，不允许负偏离，负偏离作为无效响应文件。采购文件要求有明确要求的按要求提供证明材料进行佐证，未明确要求的条款，在技术、服务应答表中响应即可，但供应商必须如实响应，自行承担相关法律责任。未按要求提供证明资料或者虽提供但无法佐证者，均自行承担被评审委员会视为技术参数负偏离的风险。

2.供应商须严格按照采购文件产品参数描述进行响应，不得曲解采购文件产品参数描述意思或以其他参数描述来响应采购文件参数，不得以“正偏离”为由偷换技术参数描述方式进行响应，否则自行承担被评审委员会视为技术参数负

偏离的风险。

3.所有证明材料均需加盖供应商公章，未盖章视为无效证明材料。