**鹤山市妇幼保健院车牌识别、监控、WiFi服务项目招标需求**

在现代化停车管理中，涉及到各方面的管理，其中车辆的管理是一个重要的方面。尤其是对医院等重要场所，要求对各种车辆惊醒严格的管理，对其出入的时间进行要严格的监视，并对各类车辆进行登记（包括内部车辆和外部车辆）和识别。对于我院，各种出入的车辆较多，每辆车都要进行人工判断，既费时，又不利于管理和查询。门卫工作比较困难，效率低下。同时有部分来外车辆长期停放在院内停车场内，无法精准对其实施管控。为了改善现时我院与现代化停车场不对称的管理模式，需要尽快实现车辆管理工作自动化、智能化，对大门进出口的车辆进行有效地，准确地管控。

随着信息技术的飞速发展和我国信息化的推进，使用有线无线局域网产品可以实现建筑群网络连接、宽带互连网络接入以及移动获取网络服务等功能。无线网络产品具有传输距离远、可以在建筑物之间或建筑物内施工困难的环境下使用、支持移动漫游等特点；随着移动设备使用的普及，人们对网络服务的要求也越来越高，现时公共审计WiFi已经是医院的标配，院内布建公共审计WiFi既能满足就诊人员和陪诊人员在等候时间内的上网需求也符合公安安全审计要求。通过公共WiFi进一步提升医院服务，给就诊人员和陪诊人员一个更加舒适的医院环境，同时自动推送满意度调测问卷，协助我院推进满意度调查方面工作。

我院已自有一套海康威视的视频监控设备，统一管理院内共112支视频监控枪。现时新建副楼已装修完工，但是副楼只有室内安装了监控枪，室外还没有布建监控。另外根据相关政府机构文件要求，我院的麻醉剂药物的存放、使用、销毁地点必须要有监控枪进行实时记录与视频必须保存180日。因此，我院需要在现有监控系统上加建相应数量的监控枪支。

1. **项目名称：鹤山市妇幼保健院车牌识别、监控、WiFi服务项目**
2. **采购内容及预算**

|  |  |  |  |
| --- | --- | --- | --- |
| **采购内容** | **数量** | **完工期** | **最高限价** |
| 鹤山市妇幼保健院车牌识别、监控、WiFi服务 | 1项 | 合同签订生效之日起60个日历日内完成货物供应、安装、调试、验收合格 | 人民币37.5万元（按合同额分36个月支付） |

1. **投标文件截止时间**

2022年5月7日（自招标文件开始发出之日起至投标人提交投标文件截止之日止，不得少于7日）。

地点：鹤山市妇幼保健院12楼信息科。（地址：广东省江门市鹤山市鹤山大道北1156号）

1. **投标人资质要求**

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求：本项目不属于专门面向中小企业采购的项目；

3、完工期：合同签订生效后 60个日历日内完成交货及安装调试。

4、投标人须有能力提供完善的售后服务(包括技术人员、响应时间及备品、备件方面等)。负责免费现场培训采购人操作人员，直至掌握操作技术为止。

5、投标人（非江门地区内注册的）必须在江门地区内设有固定的售后服务机构（必须提供相关证明材料，不接受委托第三方提供售后服务）

6、售后服务：

（1）自验收合格之日起，所投报的全部硬件产品,提供至少3年的免费保修期；保修期内免费维护，并免费提供备品、备件；所投报的软件产品提供至少1年的免费维护期，维护期内免费升级及维护。无论在保修期（维护期）内或保修期（维护期）外，投标人需提供上门服务。投标人需提供终身售后服务。

（2）设备发生故障后，自报障时起算，1小时内响应，4小时内到达现场，24小时内解决问题。如果设备故障在规定时间内仍无法排除，投标人应在随后24小时内提供不低于故障设备规格型号档次的备用设备供采购人代替使用，直至故障设备修复，确保设备的正常使用。

（3）应急响应服务：保障车牌识别、WiFi网络、视频监控等系统的核心网络设备和关键线路发生故障后能快速修复，响应时限要求：需具备7\*24小时的故障响应能力，响应时间小于40分钟,3小时内到达现场处理，故障处理时间要求：一般故障24小时内解决。如果设备硬件故障在规定时间内仍无法排除，应在随后72小时内提供不低于故障设备规格型号档次的备用设备代替使用，直至故障设备修复。

（4）服务便捷要求：1）需鹤山市内设有固定服务机构，提供固定服务机构的营业执照复印件，并加盖单位公章；2）需提供本项目服务人员一年社保正面，提供服务人员任职证明，并加盖单位公章；（模板见附件三）3）需提供本项目自有服务车辆情况说明，并加盖单位公章。（模板见附件四）

7、投标人须负责免费培训采购人的使用人员，直至完全掌握设备的操作、日常维护保养及简单维修方法。

8、付款方式：按月支付

工程验收后，按合同额分36个月支付。

9、本项目的特定资格要求：

（1）投标人应当具备《中华人民共和国政府采购法》第二十二条规定的条件；

1）投标人应当是具有独立承担民事责任能力的在中华人民共和国境内注册的法人、其他组织或者自然人；（提供有效的营业执照或相关单位登记证书复印件（若法人或者其他组织投标的），自然人有效的身份证明复印件（若自然人投标的）。若分支机构投标的，应当取得总公司（总所）出具给分支机构的有效授权，并同时提供总公司（总所）的营业执照、总公司（总所）出具给分支机构的有效授权书及分支机构的营业执照复印件。（授权模板见附件二）

2）投标人应当具有良好的商业信誉和健全的财务会计制度。（提供2020年度或2021年1月至今任意1个月的财务状况报告或银行出具的资信证明复印件）

3）投标人应当具有履行合同所必需的设备和专业技术能力。（提供《关于资格的声明函》）

4）投标人应当有依法缴纳税收和社会保障资金的良好记录。（提供2021年1月至今任意1个月的依法缴纳税收和社会保障资金的相关材料复印件，如依法免税或不需要缴纳社会保障资金的，应当提供相应证明文件复印件）

5）投标人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。重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，较大数额罚款按照发出行政处罚决定书部门所在省级政府，或实行垂直领导的国务院有关行政主管部门制定的较大数额罚款标准，或罚款决定之前需要举行听证会的金额标准来认定。（提供《关于资格的声明函》，模板见附件一）

6）投标人应当符合法律、行政法规规定的其他条件。（提供《关于资格的声明函》，模板见附件一）

（2）投标人未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单，不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间，（以开标当日采购代理机构通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询投标人信用记录为准，如相关失信记录已失效，应当提供相应证明文件复印件。

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同包项下的招标活动。（提供《关于资格的声明函》，模板见附件一）

（4）为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。（提供《关于资格的声明函》，模板见附件一）

（5）本合同包不接受联合体投标。（提供《关于资格的声明函》，模板见附件一）

1. **项目范围**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 建设细分 | 建设地点 | 建设要求 | 实现效果 |
| 1 | 车牌识别系统建设部分 | 正门与侧门 | 1、正门方向一出一入个一台，侧门方向同一条道只出不进。正门两条车道，一出一入，各配一个挡车器。侧门出入同一条车道，共用一个挡车器。 2、需满足应急车辆（消防车）正常出入。 3、扫码登记免费停车； 4、自动车牌识别功能，识别率高达 99.6%。 5、显示功能，当车辆进出时，可显示提示语、车辆、缴费等信息；支持固定二维码扫码缴费功能；语音播报功能，当车辆进出时，自动播报提示语、车辆、缴费等信息。  6、自动补光功能，当车场光线不足时，补光灯自动开启。 | 1、院大门出入双向通道，实现人车分流；车牌识别，自动进出。  2、规范化管控车辆，自定义收费（院内员工车辆免费）。3、服务对象前台登记即可免费停车。外来非服务对象超过停车规定时间则需支付相应停车费。 |
| 2 | WiFi建设部分 | 主楼与附楼 | 1、主楼和附楼相应楼层及发热门诊实现WiFi覆盖。 2、非院内人员需短信验证使用WiFi。 3、院内人员设置白名单使用WiFi。 3、可以推送满意度问卷调查。 | 1、人员无需短信验证即可使用WiFi。 2、就诊人员和陪诊人员成功登录WiFi前需短信验证并填写问卷调查。 |
| 3 | 监控建设部分 | 妇幼主楼 | 1、主楼6楼产科、主楼5楼妇科和手术室、主楼1楼药库和药房需要增加摄像枪，存储180天。优先利旧现有资源。2、附楼外围摄像枪补点。  3、重点药物监控摄像视频存储180天，附楼外围视频存储30天。 | 1、授权院内3-5个管理人员手机查看院内视频监控。 |

1. **商务要求**

1、本次招标采购内容为鹤山市妇幼保健院车牌识别、监控、WiFi服务项目（具体要求详见“技术要求”）。投标人不得将本项目中的内容拆散来投标。

2、投标人应当说明与本项目类似的其它项目的业绩和服务情况等。

3、投标人应当提供相关的财务及资信情况资料，以证明其经营状况及履约能力。

4、投标人如提供质量免检产品、节能产品、环境标志产品、小型和微型企业（监狱企业、残疾人福利单位视同小型、微型企业）产品（或服务）的，应在投标文件中提供相关证明文件。

5、投标报价应为人民币含税全包价，包括所有的费用。

6、服务地点：项目实施地点（以合同为准）。

7、本项目如涉及商品包装、快递包装，应当满足商品包装政府采购需求标准、快递包装政府采购需求标准。

8、完工期：合同签订生效后60个工作日内完成设备安装调试、开通，并能正常投入使用。

9、验收标准：以国家现行相关规范为验收标准，按时完成项目。

10、服务要求：具体要求详见技术要求。

11、投标人必须由法定代表人/负责人或委托代理人参加开标仪式，随时接受评标委员会询问，并就有关问题予以正式解答。

1. **技术要求**

（一）项目建设内容

为实现本项目对智能化系统先进性的要求，需采用先进的，具极强网络功能的、配合高保密性的智能化管理系统设备，建立一个可信赖的智能系统。本着集成化的原则，需将车牌识别系统、WiFi网络系统、监控系统建成一个安全高效、使用方便、适应力强、符合计算机和网络通信技术最新发展潮流并应用成熟的系统。

（二）设备功能及技术要求（功能质量相当或优于以下要求，本采购技术要求中凡标有“▲”的地方均被视为重要的技术指标要求或性能要求。凡标有“★”的地方均的条款为必须实质性响应，不允许负偏离（不满足要求），供应商对这些关键条款未响应或不满足的，将按无效投标处理）

1、车牌识别系统功能及技术指标参数要求

（1）车牌识别系统组成模块：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | | 说明 |
| 1 | 车牌识别控制机 | | 1. 技术参数  ▲外形尺寸：不大于206\*236.4\*1340mm（长\*宽\*高）   整机重量：<20KG   工作温度：-25℃～70℃   工作湿度：≤95%，不凝露   防护等级：IP65   ▲电源电压：AC220V±10% 50Hz   ▲额定功率：<40W   ▲ 通讯方式：TCP/IP通讯  2、相机模块可以上下左右调整角度，保证车牌在画面中处于水平位置；  3、抓拍点距离车牌识别器3～5米最佳；  4、车牌长度的像素点在140～160之间，识别效果最佳，可此为标准调节安装距离和角度等；  5、 内置补光灯的方向和角度可以调整，正确调节补光灯，可在夜间捕获更好的成像质量并提高识别率； |
| 2 | 挡车器 | | 1、技术参数   ▲工作电压：AC 220V ±10% 50Hz   ▲输出功率：≤180W   开、关闸运行时间：不同的闸杆类型匹配不同的开、关闸速度，最快 1.0秒 u  ▲运行寿命：≥500万次   温度范围：-25℃~70℃   ▲箱体尺寸：不大于300\*270\*1000mm（长\*宽\*高）  2、电机使用 DC 24V无刷电机，不会有传统道闸使用中出现的因为高速与长久运行而导致的过流、过热保护使电机停止运行； 3、双向自锁功能：  闸杆开到位时，外力不能使其下降，开闸按钮（或远程开闸信号）无效；  闸杆关到位时，外力不能使其上升，关闸按钮（或远程关闸信号）无效； 4、时间保护功能：  当限位开关失效时，通过设定合适的运行时间，可以使挡车器电机不至于长时间运转而损坏； 5、具有开优先功能，在关闭的过程中发出“开”命令，挡车器马上开启；  6、具有关记忆功能，需要时可以对其进行设置。在挡车器处于开启过程中发出该命令，当开到位时会自动关闭；  7、具有遥控接口，可以配置遥控发射器, 从而控制电动挡车器闸杆的升、降、停；  8、遥控、按钮、手动三种操作方式；  9、通电时，使用遥控发射器，由“开”、“关”、“停”三键控制；若没有遥控发射器，可由控制盒上的三个按钮来控制；  10、停电时，可手动快速起杆；来电后自动复位； |
| 3 | ▲平台 | 登记 | 给车牌发行车场权限。如果登记之前没有登记人员信息，则自动生成人员 编号，手动输入人员姓名，车牌登记完成后进入人员信息栏进行完善人员信息操作。 |
| 改写 | 针对车牌授权的通道信息、金额、车类、持有人、车场有效期等信息的改写。 |
| 延期 | 发行的临时车可进行延期操作。输入延期月数及延期金额，截止日期 自动生成，点击“延期”按钮进行延期操作。 |
| 批量改写 | 批量改写界面可对车牌的权限进行批量改写。授权按钮只能增加和删除车道权限，不会 更改车类或有效期；修改按钮可更改车道权限，也可以修改有效期，是否更改有效期的起始 时间或截止时间可勾选。 |
| 自定义批量修改 | 可根据实际需要批量修改车类、有效期起始时间、有效期截止时间、 车道权限等，勾选后才能修改，未勾选则不变。车道权限只能单独修改，可以选择新增或删 除车道权限。 |
| 更换车牌 | 输入旧车牌，调出原授权信息，再输入新车牌，点击“换牌”按钮。更换车牌后，保留 原有的授权权限，车辆下次进场生效。 |
| 车场管理 | 可进行停车场配置（车场、岗亭、车道、设备）、 车辆进出逻辑设置、收费标准加载、黑名单设置、运营管理（修正车牌、补录场内记录、删 除场内记录、车辆预约、固定车延期金额设置、优惠功能等）、工作站设置、剩余车位发布、车牌授权审核、管理员发行权限设置等 |
| 中央缴费 | 新建中央缴费工作站，配 置线上支付功能，可移动支付，通过输入车牌号进行缴费。输入车牌号时，可以进行模糊查询，选择对应的车牌号行缴费。缴费时可选择车类，线下优惠券等，可选择是否开 具纸质发票或电子发票。也可通过生成的微信或者支付宝二维码进行扫码支付。 |
| 入场信息补录 | 当车辆入场没有识别到车牌时，可以通过入场信息补录功能补录一条完整的入场信息， 补录入场信息时，要填写车牌号码、入场时间、车类、所属车道等信息。 |
| 免费登记 | 车辆必须要在场内之后才能登记，登记之后此车辆在规定时间内进出都是免费的，超出 了免费时间之后、按设置的过期收费类型的卡类算费。 |
| 二维码优惠券 | 可生成医院发放的二维码电子优惠券，或打印出二维码纸质优惠券。车辆缴费时，可使用二维码电子优惠券或扫描打印的纸质优惠券优惠出场。 |
| 明细报表 | 所有的明细报表按子系统分类展示，可在对应的明细报表中查询。可多种条件组合 查询，报表可以EXCEL、PDF、CSV 格式导出，方便打印、二次数据处理、存档等 |
| 场内车辆记录 | 从停车场入口进场且未出场的车辆信息查询。可以查看凭证号、凭证类型、车类名称、 入场时间、停车时长等等相关信息（此报表可以根据入场时间划分时间段查看） |
| 入场流水记录 | 从停车场入口进场的车辆信息查询。可以查看凭证号、凭证类型、车类名称、入场时间 等相关信息。 |
| 已出场车辆记录 | 从停车场出口已经出场的车辆信息查询。可以查看凭证号、凭证类型、车类名称、入场 时间、出场时间、收费金额等相关信息。 |
| 网络中断仍可工作 | 当服务器异常或脱网时，系统可脱离服务器自动运行，车辆仍可进出，计费，数据本地存储。待网络恢复正常后，数据自动上传，无需人工干预，保证数据的完整性。 |
| 手动开闸/非法开闸记录 | 该报表可以查询手动开闸和非法开闸的详细记录。可以查看凭证号、车类名称、创建时 间、开闸类型等等相关信息。 |

★备注：硬件设备需提供原厂授权和原厂保修三年服务承诺函。

（2）车牌识别流程说明

|  |  |  |
| --- | --- | --- |
| 序号 | 各类型车辆组织 | 流程说明 |
| 1 | ▲月卡车辆组织（医院内部人员使用） | 月租车纯车牌识别进出流程： 进场流程说明：  固定车辆驶入停车场入口，车辆压地感线圈，触发车牌识别器抓拍图像并识别车牌号码，系统记录车牌号码、入场抓拍图像、入场时间等信息，显示屏、语音提示相关信息（如车牌号码、欢迎入场、固定车辆剩余日期等）并开启挡车器，车辆入场，闸杆自动落下，车辆进入车场内泊车。 出场流程说明： 固定车辆驶到停车场出口，车辆压地感线圈，触发车牌识别器抓拍图像并识别车牌号码，系统记录车牌号码、出场抓拍图像、出场时间等信息，显示屏语音提示相关信息（如车牌号码、一路平安、固定车辆剩余日期、延期等）并开启挡车器，车辆出场，车过后，闸杆自动落下，车辆通行离开停车场。 |
| 2 | ▲临时车辆组织 | 进场流程说明： 临时车辆驶入停车场入口，车辆压地感线圈，触发车牌识别器抓牌图像并识别车牌号码，系统记录车牌号码、入场抓拍图像、入场时间等信息，显示屏语音提示相关信息（如车牌号码、欢迎入场等）并开启挡车器，车辆入场，闸杆自动落下。 出场流程说明： 临时车辆驶到停车场出口，车辆压地感线圈，触发车牌识别器抓牌图像并识别车牌号码，系统记录车牌号码、出场抓拍图像、出场时间等信息，显示屏语音提示相关信息（如车牌号码、缴费信息等）。 临时车辆不需要缴纳费用（免费）或已在中央收费处缴纳过费用，则自动开启挡车器，车辆出场，车过后，闸杆自动落下，车辆通行离开停车场。临时车辆需要缴纳费用的，完成缴费后，手动开启挡车器，车辆出场，车过后，闸杆自动落下。 临时车辆车牌号码识别有误时，需要人工操作，完成缴费后，手动开启挡车器，车辆出场，车过后，闸杆自动落下，车辆通行离开停车场。 |
| 3 | ▲无人值守车辆组织 | 1、无人值守固定车辆进出场流程说明 固定车辆进出场流程同上所述，与有人值守状况一致。 2、无人值守临时车辆进场流程说明 临时车辆驶入停车场入口，车辆压地感线圈，触发车牌识别器抓牌图像并识别车牌号码，系统记录车牌号码、入场抓拍图像、入场时间等信息，显示屏语音提示相关信息（如车牌号码、欢迎入场等）并开启挡车器，车辆入场，闸杆自动落下。 3、无人值守临时车辆出场流程说明 临时车辆驶到停车场出口，车辆压地感线圈，触发车牌识别器抓牌图像并识别车牌号码，系统记录车牌号码、出场抓拍图像、出场时间等信息，显示屏语音提示相关信息（如车牌号码、缴费信息等）。 临时车辆无费用、或已缴费且未超时，则自动开启挡车器，车辆出场，车过后，闸杆自动落下，车辆通行离开停车场。 临时车未缴费，无人值守控制机的LCD显示屏上生成缴费二维码，车主打开微信/支付宝扫显示屏二维码或打开付款二维码放置在无人值守控制机的扫描区域，付款成功后，智慧车场一体机开闸，车辆通行离开停车场。 |
| 4 | 无牌或不可识别车牌车辆车流组织 | 1、进场流程说明 车辆（无牌车）驶入识别区域，智慧车场一体机识别车辆为无牌车，语音及显示屏提示车辆请扫二维码入场；车主打开微信/支付宝扫描无人值守控制机LCD显示屏上生成的二维码，一体机开闸，车辆入场。 2、出场流程说明 车辆（无牌车）驶入识别区域，智慧车场一体机识别车辆为无牌车，语音及显示屏提示车辆“请扫二维码缴费”；算费二维码显示在无人值守控制机LCD显示屏，车主打开微信/支付宝扫显示屏二维码，系统根据微信/支付宝入场记录自动计算费用，车主付款成功后，一体机开闸，车辆出场。 |
| 5 | 特殊车辆车辆组织 | 警车、武警、教练车、军车、粤港粤澳、使领馆、民航军警车辆等特殊车辆。可根据物业管理方的需求，设置为按贵宾车辆免费自动开闸通行。也可设置为按临时车收费通行。所有车辆进出有明细报表和统计报表。 |

（3）停车费支付方式及移动支付

|  |  |  |
| --- | --- | --- |
| 序号 | 支付方式 | 说明 |
| 1 | 现金支付 | 当车辆在停车场中产生停车费用，可采用现金进行支付停车费用。 |
| 2 | ▲微信支付 | 车辆在停车场中产生停车费用，可采用微信进行支付停车费用。 停车管理物业收费单位开设微信收费账号即可实现微信收费。 |
| 3 | ▲支付宝支付 | 车辆在停车场中产生停车费用，可采用支付宝进行支付停车费用。 停车管理物业收费单位开设支付宝收费账号即可实现微信收费。 驾驶员打开其手机支付宝支付页面的“扫一扫”功能，直接扫描车场内或出口处的收费二维码，并根据提示支付停车费用； |
| 4 | 银联闪付 | 当车场中设有银联闪付设备时，车辆缴费时，可采用银联闪付支付停车费用。 |
| 5 | 无感支付高速通行 | 车主可开通微信或支付宝无感支付功能，即可在出场无需扫码缴费或付现金，识别车牌后可自动扣费并开闸出场 |

（4）停车发票形式

|  |  |  |
| --- | --- | --- |
| 序号 | 发票形式 | 说明 |
| 1 | ▲电子发票 | 当车辆缴费后，点击“去开发票”按钮，也可事后查询缴费记录进行开票；所缴金额等数据系统自动填写，且无法更改。由车主只需填写公司、接收发票邮件等信息，即可进行开票。开票成功后电子发票会自动发送到车主的邮箱中。 |

2、WiFi功能及技术指标参数要求

（1）AC控制器

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| ★管理AP数 | 支持常规AP最大数量≥128 |
| ▲端口要求 | LAN:8\*GE  WAN:2\*2.5GE  10GBASE-R-SFP+口2个  USB≥1个 |
| ▲转发性能 | 集中转发性能≥4Gbps |
| 组网能力 | 支持标准IETF 5415 CAPWAP协议，AP和AC之间支持L2/L3层网络拓扑，为提高网络安全，AP与控制器之间能够支持DTLS对CAPWAP隧道进行加密处理。 |
| ▲认证加密 | 支持MAC 地址认证、802.1x认证（EAP-PAP、EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS）、Portal认证、MAC+Portal混合认证；  支持WPA标准、WEP(WEP64/WEP128)、TKIP、CCMP；  支持内置portal、dot1x服务器；  支持Private PSK方式的动态密码功能，可以为每终端分配独立秘钥。  支持WPA3个人级方式下的终端接入；支持WPA3企业级模式下的终端接入功能。  支持防PSK暴力破解，当用户密码错误超过预设的阀值之后，能够将该用户加入动态黑名单，一段时间内禁止其接入网络 |
| 无线漫游 | 支持AC内漫游，支持跨AC间漫游，支持跨VLAN的三层漫游  支持基于802.11k/802.11v/802.11r协议的智能漫游 |
| 可靠性 | 支持雷达检测SSID逃生功能：AC、AP支持SSID自主逃生，当AP射频检测到雷达信号时，会将本射频的SSID迁移到其他射频，保障关键业务正常通信。  MAC认证逃生功能：AC、AP支持MAC认证逃生功能，为提高无线网络认证可靠性，无线控制器支持MAC认证逃生功能。  支持Dot1x认证逃生功能：AC、AP支持Dot1x认证逃生功能，为提高无线网络认证可靠性，无线控制器支持Dot1x认证逃生功能。  支持Portal认证逃生功能：AC、AP支持Portal认证逃生，为提高无线网络认证可靠性，无线控制器支持Portal认证逃生功能。  支持RemoteAP功能：AC、AP支持RemoteAP功能，为提升无线网络的可靠性，AP具备逃生功能，当AC不可达造成AP离线时，AP能够继续维持原有用户不下线，新用户仍可以接入网络保证业务正常。支持认证用户和非认证用户。 |
| 认证加密 | 支持Portal在线用户与DHCP租约联动功能：AC支持根据DHCP租约信息联动Portal用户自动下线，可以提高DHCP地址池的利用率，降低Portal重复认证开销。  能够有效拦截Portal用户重定向攻击 |
| ▲无线运维 | 为监控AP有线端口异常所引起的无线网络体检较差的原因，所投产品需要支持：有线端口接收错包持续增长、AP有线端口Down、有线端口协商速率低、有线端口发送错包持续增加、有线端口协商成半双工等问题的检测，需要提供功能截图证明  为实现AC的全面运维，所投产品需要支持：AC CPU、内存使用率以及历史信息，AC整机广播、组播、单播流量成分以及历史信息，AC仿真面板端口图以及每端口广播、组播、单播流量成分以及历史信息，同时可以识别最近一分钟端口入方向广播组播占比过高、最近一分钟端口流量过大等异常事件，需要提供第三方认证报告证明（绿洲智能运维报告）  为识别因IP地址获取异常造成的用户体验差的情形，所投产品需要支持终端IP地址获取失败、终端IP地址获取超时、终端IP获取慢等异常数量统计，并给出问题分布趋势图、该问题所影响的具体终端，涉及的AP以及该AP发生该异常的数量统计，需要提供第三方认证报告  为精准识别终端接入过程中存在的异常，所投产品需要图形化呈现终端在关联、802.1x认证、PSK认证、IP地址获取等阶段的全部协议交互流程及各个阶段的耗时，要求提供第三方认证报告证明  为保障重要用户的无线网络体验，所投产品需要支持VIP功能，并图形化展示VIP用户速率、延时、平均信号强度等无线体验信息，要求提供截图证明  为使得网络管理员实时感知网络状态，所投产品需要在网络发生异常时，可利用短信、微信、邮件等三种不同方式推送告警信息，要求提第三方认证报告证明  为分析无线网络中IP地址的异常改变造成的上网体验差的原因，所投产品需要支持对异常终端的IP地址变更时间、MAC地址、IP地址、接入SSID以及接入AP信息予以记录及显示，需要提供第三方报告证明  为了有效分析无线网络通信质量，所投产品需要统计终端首次接入互联网的时长，要求提供第三方认证报告证明。  为了有效排查无线网络中存在的匿名攻击的隐患，所投产品需要具备仿冒终端检查的能力，并且识别仿冒终端所接入SSID、AP以及终端设备型号、终端操作系统等信息，要求提供第三方认证报告证明  为了保障无线网络的用户体验，所投产品需要支持对弱信号接入、乒乓漫游等常见无线网络问题的识别，并给出问题分布趋势图、该问题所影响的具体终端、涉及的AP以及该AP发生该异常的数量统计，需要提供第三方认证报告证明。 |
| ▲进网许可证 | 要求提供所投设备进网许可证 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（2）普通型AP发射器

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| ★工作模式 | 可支持瘦AP工作模式，支持802.11ac协议，支持WiFi6 |
| MU-MIMO | 支持MU-MIMO |
| ▲协议支持 | 802.11a/n/ac : 5.725GHz-5.850GHz (中国)  802.11b/g/n : 2.4GHz-2.483GHz (中国) |
| ▲工作频段 | 2.4GHz和5GHz |
| ▲接口 | ≥2个10/100/1000Mbps(RJ45)，双网口PoE供电、支持端口负载均衡 |
| ▲发射功率 | ≥20dBm |
| 空间流数 | ≥4 |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 天线 | 内置天线 |
| 功耗 | 整机最大功耗≤12.5W |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 终端感知准入 | 支持 |
| 用户隔离 | 支持AP上二层转发抑制 |
| 支持虚拟AP(多SSID)之间的隔离 |
| ▲运维平台 | 该产品厂家需提供免费云端维护平台，并提供免费手机APP管理软件，投标方需提供云端维护平台及手机APP软件的截图。 |
| ▲运维平台及APP功能 | 配合无线控制器，可以实现定期巡检，通过收集网络的各种关键指标，包括信道利用率情况，丢包率，时间延迟，包重传次数，漫游成功率，终端信号强度等，统计健康度得分，输出体检报告，并结合报告，给出优化建议。  手机APP配合无线控制器，可以展现网络健康度监测各方面指标,及时定位网络问题,并通过数据库支持，保障问题实时处理。投标方需提供该功能截图。 |
| 认证 | 配合无线控制器，可以实现包括公众号认证、微信连WIFI、固定账号认证、短信认证等多种认证方式，实现广告推送，粉丝营销。  可以设置允许上网的时长，闲置切断，以及认证成功后跳转URL，支持开启免认证（认证成功后无需再次认证）， |
| 无线链路层安全监控防御(WIPS) | 能够基于SSID发现和抑制非法AP，一些非法AP仿冒合法SSID提供WLAN接入服务,干扰网络正常运营。能够检测WLAN覆盖合法AP下的非法用户或者非法终端对无线AP进行攻击并产生告警给AP管理平台。  基于WIPS的钓鱼AP检测，不法人员通过仿冒SSID，或者相近的SSID,引诱合法用户来连接，盗取账号信息。 |
| 无线物理层安全监测功能（频谱防护） | 配合无线控制器能够协同网管提供频谱防护图表，并且所显示的频谱防护内容同时包括2.4GHz频段和5GHz频段的快速变换(FFT)以及信道占空比等无线频谱实时动态图表。  当开启蓝牙设备、微波炉等非WiFi干扰设备时，频谱防护管理界面中可以在快速变换(FFT)以及信道占空比等无线频谱实时动态图表直观地显示出干扰信号对信道质量造成的影响，并且能够在干扰设备列表中识别出干扰源的类型； |
| 智能带宽限速 | 基于带宽均分算法 |
| 基于每用户指定带宽的算法 |
| 在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 报文过滤 | 支持 |
| 管理 | 支持TR-069、SNMP V1/V2c/V3、Trap、HTTP(S) 、SSH、Telnet、FTP/TFTP |
| QoS策略映射 | 支持不同SSID/VLAN映射不同的QoS策略 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（3）高密型AP发射器

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| ★工作模式 | 采用整机双频3流设计，可同时工作在802.11a/b/g/n/ac/ac wave2/ax模式，支持WiFi6 |
| MU-MIMO | 所有射频都支持MU-MIMO |
| ★协商速率 | 整机协商速率≥1.487Gbps |
| 天线设计 | 要求采用内置智能天线设计 |
| 接口设计 | ≥1个10/100/1000Mbps(RJ45) |
| 空口优化 | 支持基于空口利用率的SSID自动隐藏功能，当空口繁忙程度达到或超过配置的阈值时，SSID自动隐藏，为用户提供稳定可靠的无线服务。 |
| 接入安全 | 支持WPA3个人级方式下的终端接入；支持WPA3企业级模式下的终端接入功能。 |
| 接入规格 | 整机接入用户规格1024，要求提供官网链接以及官网截图证明，保留测试权力 |
| ▲WIFI联盟证书 | 为保证终端互联互通有效性，投标投标厂家需提供投标产品WiFi联盟证书 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（4）接入交换机

| 功能及技术指标 | 详细技术参数 |
| --- | --- |
| ▲交换容量 | ≥256Gbps |
| ▲转发性能 | ≥30Mpps |
| ▲性能指标 | MAC地址表>=8K |
| ▲POE | 支持POE+，≥190W |
| 端口形态 | 8个10/100/1000Base-T以太网端口，2个1000Base-X以太网端口 |
| 以太网特性 | 流控(802.3x)  绿色以太网（EEE）  端口自动节能  动态链路聚合(802.3ad)/ 静态端口聚合  802.1p、802.1Q  电缆诊断  STP(802.1D)/ RSTP(802.1w)/ MSTP(802.1s)  TC snooping  BPDU 保护/根保护/环回保护/防TC-BPDU攻击保护功能 |
| IPv4 | ARP  DHCP Client |
| 组播 | 支持IGMP V1/V2/V3 Snooping  支持快速离开机制 |
| QoS | 支持Diff-Serv QoS  支持SP/WRR/SP+WRR  流量限速  802.1p/DSCP优先级映射优先级映射 |
| 安全性 | 用户分级管理  黑洞MAC  端口 MAC地址学习数限制  SSL |
| 网管和监控 | WEB页面配置  FTP、TFTP、Xmodem文件上下载管理 |
| 系统管理 | 支持Console/AUX Modem/Telnet/SSH2.0 命令行配置  支持FTP、TFTP、Xmodem、SFTP文件上下载管理  支持SNMP V1/V2c/V3  支持NTP时钟  支持系统工作日志  支持集群管理 |
| 红口功能 | 支持将设备前几个端口使能红口，获得优先转发的能力，  保证高可靠业务需求的稳定；  提供设备红口标注图片； |
| ▲资质认证 | 要求提供检验报告 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（5）汇聚交换机

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| ▲交换容量 | ≥2.56Tbps |
| ▲转发性能 | ≥480Mpps |
| 扩展插槽数 | ≥1 |
| 电源 | 模块化双电源 |
| 性能指标 | ▲MAC地址表（max）≥32K |
| ▲路由表容量（max）≥16K |
| ▲ARP：16K |
| ▲ACL：1K（入）/256（出） |
| 接口类型 | 端口形态： |
| 24个1/10G SFP Plus端口，1个slot扩展插槽，两个电源插槽 |
| VxLAN | 支持VxLAN二层网关  支持VxLAN三层网关  支持EVPN |
| \*堆叠 | 最大堆叠台数≥9台 |
| 最大堆叠带宽≥160G |
| 可要求堆叠带宽，并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块 |
| 支持跨设备链路聚合，单一IP管理，分布式弹性路由 |
| 支持通过标准以太端口进行堆叠（万兆或40G均支持） |
| 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预 |
| 支持远程堆叠 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)≥4094 |
| 链路聚合 | 支持最多16个端口聚合；支持最多128个聚合组；支持LACP |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 组播协议 | 支持IGMP v1/v2/v3，MLD v1/v2 |
| 支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 |
| 支持PIM Snooping |
| 支持MLD Proxy |
| 支持组播VLAN |
| 支持PIM-DM，PIM-SM，PIM-SSM |
| 支持MSDP，MSDP for IPv6 |
| 支持MBGP，MBGP for Ipv6 |
| 路由协议 | ▲支持IPv4静态路由、RIP V1/V2、OSPF、BGP、ISIS |
| ▲支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)； |
| 支持RRPP（快速环网保护协议），环网故障恢复时间不超过200ms； |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 支持基于端口和VLAN的 ACL； |
| 支持IPv6 ACL； |
| 支持出方向ACL，以便于灵活实现数据包过滤； |
| 支持802.1x认证，支持集中式MAC地址认证； |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换，需提供官网网站命令手册佐证支持多控制器（EQUAL模式、主备模式）； |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |
| 支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（6）光模块

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 千兆多模 | ▲光模块-SFP-GE-多模模块-(850nm,0.55km,LC) |

★备注：硬件设备需提供原厂授权和原厂服务承、售后服务诺函。

（7）AP分布点（分布点根据医院需要在院内部署）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地点 | AP数量 | 单位 | 位置 | 备注 |
| 主楼一层 | 3 | 个 | 东中西各一个 | 高密型 |
| 主楼二层 | 2 | 个 | 东西各一个 | 高密型 |
| 主楼三层 | 2 | 个 | 东西各一个 | 高密型 |
| 主楼四层 | 2 | 个 | 东西个一个 | 高密型 |
| 主楼十层 | 1 | 个 | 东边一个 | 普通型 |
| 主楼十一层 | 1 | 个 | 东边一个 | 普通型 |
| 主楼十二层 | 2 | 个 | 东西各一个 | 普通型 |
| 主楼十三层 | 1 | 个 | 西边一个 | 普通型 |
| 辅楼1层 | 1 | 个 | 物资库 | 普通型各一个 |
| 辅楼2层 | 2 | 个 | 大厅和走廊 | 高密型和普通型各一个 |
| 发热门诊室 | 1 | 个 | 发热门诊中厅 | 高密型 |
| 门卫室 | 1 | 个 | 门卫室 | 普通型 |
| 总数 | 19 |  |  |  |

（8）安全网关

|  |  |
| --- | --- |
| 功能及技术指标 | 参数说明 |
| 接口类型 | ▲8 个千兆 电接口、2 个Combo 口、2 个Bypass 接口、2 个USB 接口、1 个Console 口以及 1 个硬盘槽位 |
| 硬件Bypass 功能 | 支持内置Bypass 接口。满足设备二层部署时，设备断电后，网络不中断的需求，保证用户业务的连续性和稳定性。 |
| 安全策略规则 | 安全策略对报文的控制可通过安全策略规则实现的，规则中可以设置匹配报文的过滤条件，处理报 文的动作和对于报文内容进行深度检测等功能。 |
| ▲入侵检测系统 | 深度防护：可以检测报文应用层的内容，以及对网络数据流进行协议分析和重组，并根据检测结果来对报文做出相应的处理。 实时防护：实时检测流经设备的网络流量，并对入侵活动和攻击性网络流量进行实时拦截。 全方位防护：可以对多种攻击类型提供防护措施，例如蠕虫、病毒、木马、僵尸网络、间谍软 件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具、后门等。 内外兼防：对经过设备的流量都可以进行检测，不仅可以防止来自企业外部的攻击，还可以防止发自企业内部的攻击。 不断升级，精准防护：保证每周两次的例行 IPS 特征库更新和24 小时的紧急更新响应，紧急更新响应可以用短信或者Email 通知到网管本人。 自定义IPS 特征：管理员在设备上手工创建。通常新的网络攻击出现后，与其对应的攻击特征会出现的比较晚一些。如果管理员已经掌握了新网络攻击行为的特点，可以自己定义或者装载 第三方的攻击规则，及时阻止网络攻击 |
| ▲海量病毒防护 | 支持百万级别的病毒识别，具备高识别率和开启防病毒时设备的高处理性能。同时， 天翼安全网关还支持病毒云查杀功能。流经设备的报文首先会与该防病毒策略中的规则匹配。如果 匹配失败并且在防病毒策略中使能云端查询功能，则触发云查询。 |
| URL分类过滤 | 设备本地URL库： 提供海量预分类的URL 地址库，可根据URL 类别实现URL 过滤，同时支持联动云端 URL 地 址库进行全面实施核查。 用户自定义URL： 用户可根据具体需求自定义新的URL 地址和 URL 分类。只要流量习惯定位较准，本地URL 库在第一个小时就可以对用户的 99%以上的 Web 访问进行成功分类。 |
| ▲带宽管理 | 带宽策略可以对符合匹配条件的流量应用带宽通道，在带宽通道中可以配置带宽保证和带宽限制功 能，进而提高带宽利用率以及在线路拥堵时保证关键业务的正常运行。 |
| ▲敏感信息保护 | 1、支持丰富的协议类型：HTTP、FTP、RTMP、POP3、SMTP、IMAP、SMB、NFS 等； 2、支持对敏感信息的过滤：如身份证号、手机号、银行卡号、信用卡号等，也可以根据用户实际 使用需求自定义敏感信息关键字； 3、文件过滤支持根据真实内容进行文件识别功能，而不是简单的根据文件后缀过滤，防止攻击者 变更文件类型逃避安全检测； 4、实现支持压缩文件内部文件再识别功能和支持解压缩文件长度功能。 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（9）网络出口

▲2条千兆宽带，一主一备接入。

3、监控建设功能及技术指标参数要求

（1）摄像枪

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 摄像枪 | ▲400万 星光级 1/3" CMOS ICR红外筒型网络摄像机（PoE款）2560 × 1440 @25 fps/1个内置麦克风/红外照射距离最远可达30 m/IP66防尘防水设计 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（2）网络录像机参数

|  |  |
| --- | --- |
| 功能及技术指标 | 参数说明 |
| 网络录像机 | ▲（1）解码性能强劲，全系列支持16路1080P解码； （2）专为高分辨率相机接入所打造，最大支持800万相机接入； ▲（3）硬盘支持全面升级，支持满配8T硬盘，进一步延长录像时间； ▲（4）平台接入协议丰富，支持萤石、Ehome以及GB28181协议，轻松实现平台接入； （5）HDMI/VGA/报警口/串口等接口一应俱全，满足各类外设接入需求；▲(6)2U 标准机箱，支持机架安装；•8盘位，最大支持8TB硬盘•支持1个HDMI 4K输出 +1个VGA异源高清1080P输出•支持8路1080P解码•支持H.265、H.264混合解码，最大支持接入8MP高清IP•2个千兆网口•自带16进4出报警口•2个USB2.0接口+1个USB3.0接口 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（3）接入交换机参数

|  |  |
| --- | --- |
| 功能及技术指标 | 参数说明 |
| 接入交换机 | ▲9口百兆PoE二层非网管交换机，8个百兆PoE电口+1个百兆电口 |

★备注：硬件设备需提供原厂授权和原厂服务、售后服务承诺函。

（4）摄像枪安装位置：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地点 | 摄像枪数量 | 设备厂家 | 存储天数 | 备注 |
| 主楼6楼产科 | 2 | 海康威视 | 180天 | 新装摄像枪 |
| 主楼5楼妇科和手术室 | 2 | 海康威视 | 180天 | 新装摄像枪 |
| 主楼1楼药库和药房 | 0 | 海康威视 | 180天 | 摄像枪利旧现有两支接入项目录像机 |
| 副楼外围 | 4 | 海康威视 | 30天 | 新装摄像枪 |
| 汇总： | 8 |  |  |  |

1. **项目服务保障**

提供完善的售后服务和技术支持方案，包括但不限于以下内容：

1、 远程维护：包括电话、E-mail、远程登录等方式，提供每周7×24小时服务。

2、 现场维护：中标服务方按照招标方需求，派遣技术人员到医院指定现场提供技术支持服务。

1. **保密责任**

中标服务方在获取到医院有关数据库、服务器、远程登录、网络设备口令、数据信息等涉密内容时，不得透露给第三方，以上设备信息安全保密及其他要求要符合国家标准，如在保修期内（三年）需要整改的，承建方要无条件完成相关整改，否则给医院造成损失应追究经济和法律责任，赔偿金额不受本合同其它条款的制约。

附件一：资格声明函

**资格声明函**

**致：XXX保健院**

关于贵方采购项目名称：**XXX项目**采购项目编号：**XXX**的招标邀请，本签字人愿意参加投标，提供投标文件中规定的货物及服务，并证明提交的下列文件和说明是准确的和真实的。

1、我方为本次投标所提交的所有证明其合格和资格的文件是真实的和正确的，并愿为其真实性和正确性承担法律责任；

2、我方**具有** 独立承担民事责任的能力，在法律上、财务上和运作上完全独立于**XXX保健院**

（采购人）；

3、我方在参加本次招标前三年内，在经营活动中**没有**重大违法记录；

4、我方**具备**履行合同所必需的设备和专业技术能力；

5、我方**无**被列入失信被执行人、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；

6、我方**无**单位负责人为同一人或者存在直接控股、管理关系的不同投标人参加同一合同项下的采购活动；

7、我方**无**为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务,我方如果为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，就不再参加该采购项目的其他采购活动；

8、我方**具备**《政府采购法》第二十二条规定的条件。

9、我方**不是**联合体投标，且不转包和不分包。

10、我方**具备**法律、行政法规规定的其他条件。

**投标人法定代表人/负责人（或法定代表人/负责人授权代表）签字并盖公章：**

**日期：** 年 月 日

附件二：

**法定代表人/负责人资格证明书及授权委托书**

**（1）法定代表人（负责人）证明书**

现任我单位 职务，为法定代表人（负责人），特此证明。

有效期限：

附：代表人性别： 年龄： 身份证号码：

注册号码： 企业类型：

经营范围：

投标人（公章）：

地 址：

法定代表人（负责人）（签字或盖章）：

职 务：

**附：法定代表人（负责人）身份证复印件**

**（2）法定代表人（负责人）授权委托书**

致：

本授权书声明： （姓名）是注册于 （地方）的

（公司）的法定代表人（负责人），现任 职务，有效证件号码： 。现授权 （姓名）作为我公司的全权代理人，就项目的报价和合同执行，以我方的名义处理一切与之有关的事宜。

本授权书于 年 月 日签字生效，特此声明。

投标人（公章）：

地 址：

法定代表人（负责人）（签字或盖章）：

职 务：

被授权人（签字或盖章）：

职 务：

**附：被授权人身份证复印件**

附件三:服务人员任职证明

|  |  |
| --- | --- |
| 姓名： | 身份证号： |
| （身份证正面） | （身份证反面） |
| 姓名： | 身份证号 |
| （身份证正面） | （身份证反面） |

以上人员现任职于： （公司） 以此证明。

**法人/授权代表签字及盖公章：**

附件四：自有服务车辆情况说明（共XX辆）

|  |  |
| --- | --- |
| （行驶证） | （车辆照片，需见到车牌） |
| （行驶证） | （车辆照片，需见到车牌） |
| （行驶证） | （车辆照片，需见到车牌） |
| （行驶证） | （车辆照片，需见到车牌） |

**法人/授权代表签字及盖公章：**