**第五章 合同文本**

## 合同样本

**广州市公安局指挥中心2024年移动警务通信服务采购项目**

**服务合同**

甲方（甲方）：

乙方（乙方）：

根据《中华人民共和国民法典》，甲乙双方就广州市公安局指挥中心移动警务通信服务采购项目，经双方协商一致，共同达成如下条款：

一、甲方委托乙方进行技术服务的内容如下：

（一）服务的目标：推动警务工作移动化办理，提升一.线民警的工作效率。

（二）服务的内容：173个用户三年的移动警务通信服务。主要包括：

1.采购173个用户的移动警务通信服务。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **数量** | **备注** |
| 1 | 双系统移动警务终端 | 173台 | 运行内存不低于8G，存储量不低于256G的移动警务终端，提供3台同款（含通信套餐）（保存在采购人处）用于维修替代。 |
| 2 | 5G专网通信服务套餐 | 173套 | 套餐要求保留原有在用号码，每月包含全国不限流量（不低于20GB降速），不低于500分钟国内语音通话和不低于100条短信（超出每月套餐部分，乙方承诺以通话不高于0.19元/分钟、短信不高于0.1元/条进行结算）。如非原号码运营商中标，新乙方应在45个日历日内协调原号码运营商配合办理转网手续。 |
| 3 | 移动警务安全智能薄膜卡 | 173套 | 提供不少于安全智能薄膜卡服务总数量的2%张（3张）同款安全智能安全卡（保存在甲方处）用于维修替代，同时原在用安全智能薄膜卡保留为备份薄膜卡。 |
| 4 | 终端管控软件（MDM） | 173套 | 定制移动警务终端管理软件及部署承载后台管控平台的相关服务器硬件、网络环境及系统软件环境。部署移动警务终端集中管理的后台管控平台，并与省厅管控平台级联。 |
| 5 | 移动警务整体运维服务 | 1项 | 提供173户移动警务的整体运维服务 |

2、在服务期内提供173个5G/4G无线专网接入用户账号，并要求账号与手机卡号一一对应，非本号码操作无法使用该账号登陆内网系统，173个要求保留原有在用账号。

3、4G/5G信号须覆盖广州市行政区域，在无5G信号区域可自动切换至4G或3G网络使用，在5G网络信号不佳的使用环境，乙方应承诺提供网络优化的服务。

4、提供终端设备移动通信服务套餐，要求语音实现本次项目的173个号码广州市内免费互打，由此产生的费用由乙方自行承担，全国接听免费。

5、本次项目的173个号码，要求保留原有在用的MDM功能及原号码，且该批号码如需进行携号转网，涉及到的费用由乙方承担。

6、乙方须保证，本项目所有数据存储介质（包括硬盘、SD卡等）故障不回收。投标人需保证服务期内终端故障时乙方须在采购人监督下开展维修工作。

7、本次项目的移动警务终端通信服务到期后，乙方需承诺根据采购人需求免费提供终端及安全智能薄膜卡给甲方使用。项目到期后服务自动终止，如甲方不需要继续使用，乙方承诺需协助终端、安全智能薄膜卡以及相关敏感信息进行销毁、回收。信息脱敏工作需由具备相关资质的企业承担，所涉及费用由乙方承担。

8、如甲方在服务期间出现终端遗失情况，乙方承诺协助甲方进行终端与安全智能薄膜卡补采。

9、因通讯要求更高的可靠性、保密性，乙方需提供加密通信服务，其中要求提供的SIM卡具有商用密码产品认证证书，提供的加密通话系统/平台具有信息系统安全等级保护备案证明、具有商用密码应用安全性评估报告/商用密码检测证书及具有信通院办公即时通信软件安全能力证书。

10、出于安全备份考虑，乙方为本项目提供新的173套加密卡移动警务安全智能薄膜卡，同时需保留原有在用旧加密卡，新旧加密卡互为备份。

**（三）项目工期要求**

项目工期要求：自合同签订后，在2024年9月1日前完成173个用户的移动警务通信服务套餐（含配套的所有设备、备用设备）的供货、系统安装和调试及办妥携号转网业务（如有）；自合同签订后负责对甲方的终端进行维护；项目服务周期自所有设备完成供货并验收通过之日起计算，整体服务期限为3年。

**（四）项目实施地点**

实施地点：甲方指定地点（广州市）。

**（五）项目技术参数要求**

**5.1移动警务终端技术要求**

移动警务终端需符合公安部关于手持式移动警务双模式终端的有关规定，并需具备国产自主知识产权的操作系统。

移动警务终端要求含移动警务安全智能薄膜卡，安全智能薄膜卡经国家密码管理局批准，配用国家算法，能够与广州市公安局后台进行互通工作。

所投标设备应能兼容并正常运行目前广州市公安局在用的主流APP包括“广州警信”、“人脸识别”、“核查通”、“综合查询”、“OA”、“社区警务”、“800M对讲”、“信大客户端”、“三所客户端”、“巡逻盘查”等应用。

**5.1.1双系统移动警务终端173台**

采用手机厂商定制的双系统，分为安全系统和普通系统；在安全系统内安装警务移动专网认证的客户端和认证安全智能薄膜卡，运行警务移动专网，实行安全注册，人与手机绑定的方式，可以保证手机终端的安全使用和安全认证；在普通系统内，可安装互联网端的警务移动应用。双系统独立运行不同的网络，安全系统运行警务移动专网，普通系统运行互联网；双系统之间严格保持数据独立。

**5.1.1.1双系统移动警务终端硬件技术参数**

1）CPU：国产芯片。

2）双卡：双卡双待，主副卡不区分卡槽，支持Nano SIM卡。

3）屏幕尺寸：触控式屏幕≥6.69英寸。

4）屏幕色彩：≥10.7亿色，P3广色域

5）分辨率：≥2688 × 1216像素

6）运行内存：（RAM）≥12GB

7）机身内存：（ROM）≥256GB

8）最大支持扩展：存储卡扩展（最高支持256GB）

9）主摄像头：不低于三摄，相当于或优于5000万像素像素，支持OIS光学防抖，支持光学变焦。

10）前置摄像头：≥1300万像素（超广角，f/2.4光圈）

11）内置通信模块：支持电信、移动或联通三大运营商的移动数据网络，可通过软件对WIFI功能进行限制。支持5G/4G/3G/2G信号切换，在无5G信号区域可自动切换至4G或3G网络使用。

12）电池容量：优于或相当于4750mAh（典型值）。

13）按压式指纹传感器、360度指纹识别；息屏解锁、文件加密；

14）防root安全加固、防攻击熔断保护、安全区端口锁定；

15）带NFC功能，提供手机NFC二代身份证信息读取功能的二次开发接口和相关使用例子的源码，并对采购人的二次开发提供相关技术支持；

16）支持北斗定位系统，可获取基站定位信息；

17）系统切换：系统支持指纹及一键快速切换秒级切换；

18）开机校验：手机在面临硬件破解情况下需经与初始状态校验合格后才能启动；

19）熔断机制：芯片在面对极端攻击时可自毁，保证信息安全

20）操作系统：双独立系统，双系统同时在线，双系统文件完全隔离，安全系统apn锁定，互联网系统apn部分放开，乙方必须按照甲方所提供的应用程序APP对办公终端的操作系统进行调试，确保甲方应用程序APP可在设备上正常运行。

**5.1.1.2双系统移动警务终端软件功能技术参数**

|  |  |  |
| --- | --- | --- |
| **序号** | **需求标题** | **需求描述** |
| 1 | 系统要求 | 采用双系统方式实现，一个系统为安全系统，一个为互联网系统 |
| 2 | 要求两个系统完全隔离，数据不能共享(SIM卡中保存的数据除外)；两个系统的配置各自独立，互不影响 |
| 3 | 两个系统的应用完全独立，互不影响 |
| 4 | 两个系统预置，任何一个系统不能删除、创建或控制另外一个系统 |
| 5 | 对于此定制机型，只能刷定制的双系统ROM包，不能刷其他ROM包 |
| 6 | 系统需要防root |
| 7 | 电话要求 | 两个系统都能接电话。当前在哪个系统接电话，通话记录保存在哪个系统。通话过程不能切换系统 |
| 8 | 两个系统都能支持CDMA以及GSM双卡双待通话，LTE数据能够自动回落到CDMA、CDMA可自动升LTE |
| 9 | 短信要求 | 两个系统都能收短信，当前在哪个系统，短信属于哪个系统。两个系统短信相互独立存储，相互不能访问 |
| 10 | 通信录的要求 | 两个系统通信录相互独立，不能相互访问。如当前在互联网系统来电，互联网系统电话本没来电号码记录，则即使在安全系统中有记录，来电也只能显示号码，不能显示来电人名称 |
| 11 | 安全系统数据  业务要求 | 安全系统采用独立的APN，只能通过VPDN接入专网做数据业务 |
| 12 | APN接入点中身份验证类型默认为pap or chap，可修改。名称，代理，端口等其他设置可修改，并采用默认设置 |
| 13 | vpdn要求在运营商的2G/3G/4G/5G各制式的网络切换时，程序自动拨号联网，不需要用户手工点击开关来联网 |
| 14 | vpdn要求进入安全系统时，后台自动拨号连接，用户不感知 |
| 15 | vpdn支持可配置，配置的参数包括但不限于：APN名称，用户名，密码，鉴权类型，IP地址类型 |
| 16 | 安全系统的GSM关闭数据，只保留通话，不支持彩信 |
| 17 | 双系统数据同时在线要求 | 场景包括安全系统VPDN接入网络，同时互联网系统的WIFI或者移动数据接入网络。 |
| 18 | 支持双系统同时在线，当前系统应能够看到另外一个系统的通知栏消息，但不能看到数据 |
| 19 | 外部接口屏蔽  要求 | 安全系统的BT/互联网禁止，USB只保留充电功能。互联网系统不做限制 |
| 20 | 安全系统支持nfc读卡功能，但禁止传输数据，互联网系统不对nfc做功能限制 |
| 21 | OTA升级功能 | 整个系统通过生活区OTA更新 |
| 22 | 密码的要求 | 两个系统可以分别设置密码，指纹等。要求锁屏密码和进入系统时密码统一，只需要输入一次密码。 |
| 23 | 系统切换的要求 | 锁屏状态下，可以切换系统，必须输入当前系统的解锁密码才能进入 |
| 24 | 提供切换系统、禁止切换系统、解除禁止切换系统的接口，供有权限的第三方app调用 |
| 25 | 截屏，录屏要求 | 两个系统均提供截屏录屏接口，但是截屏，录屏的数据只能保存在用户当前操作的系统中，另一个系统不能访问。 |
| 26 | 加密卡 | 生活系统下禁用加密卡，保证安全系统下VPDN安全链路的连接。 |
| 安全系统下加密卡隐藏（隐藏后在本地文件下无法看到加密卡，其他软件无法调用。） |

**5.1.2移动警务安全智能薄膜卡173套**

移动警务终端配套，移动警务安全智能薄膜卡。具体参数要求如下：

**5.1.2.1性能指标**

1. RSA 密钥对生成（1024）：≥2.4s/对；
2. RSA 签名/解密（1024）：≥8.5次/s；
3. RSA 验证/加密（1024）：≥29.9 次/s；
4. RSA 密钥对生成（2048）：≥19s/对；
5. RSA 签名/解密（2048）：≥2.2次/s；
6. RSA 验证/加密（2048）：≥15.2次/s；
7. SM2 密钥对生成：≥0.24s/对；
8. SM2 签名/解密：≥2.6次/s；
9. SM2 验证/加密：≥2.1次/s；
10. SM3：≥7.1次/s；

**5.1.2.2物理特性**

存储器保存：至少10年；

存储器擦写次数：至少100000次；

运行环境温度：-25℃到+85℃；

存放环境温度：-40℃到+125℃；

内置国密局密码芯片，能够跟平台网关加密通讯；

加密卡支持 SM1、SM2、SM3、SM4 等国密算法；

加密卡可存储个人数字身份证书和签名私钥，为移动终端提供数字签名、签名验证和数据加密等密码服务；

加密卡可实现SM2算法和密匙管理，为移动终端提供基于SM2算法的数据加解密服务；

能够与广州市公安局移动警务安全接入平台进行互通，SIM卡与安全智能薄膜卡为各自独立的卡体，可以通过贴片的方式贴合在一起插在同一卡槽。

**5.2通讯网络要求**

移动警务终端在进行数据传输时，利用移动互联技术接入5G无线网络中的服务提供节点。提供无线专网数据配置服务，确保各移动终端使用基于5G高速分组数据网络，利用隧道技术构建与公众互联网隔离的虚拟专用网络。各移动终端通过无线专用网络安全地访问广州市公安局警务管理应用系统。通过编码技术、网络层的加密以及采用口令保护、身份验证、权限设置等措施，保证数据的完整性、避免被非法窃取区公安警务管理服务系统数据。

在无5G信号区域可自动切换至4G或3G网络使用，在5G网络信号不佳的使用环境，乙方应承诺提供网络优化的服务；对甲方在广州市内的办公场所进行5G信号覆盖，5G网络信号不佳的地方，应承诺完成包含现场施工手段在内的信号加强与网络优化服务。乙方需建立网络优化实时对接机制,在互联网提供App，支持用户发现5G信号覆盖盲区时登陆该App一键上报功能，乙方限期对上报情况反馈整改,承诺完成包含现场施工手段在内的信号加强与网络优化服务以及即时架设基站进盲。

在满足基于互联网数据传输的基础上，还需根据甲方要求，在甲方不另外支付费用的前提下随时实现：该节点保障只有合法授权的专网用户才能通过移动网络接入广州区公安内网，同时保证在合法授权的专网用户和广州公安内网内部服务器间传送的数据包不被黑客从公网非法截取，要求通过安全通道接入网络运营商路由器。乙方需承诺所提供的通信服务不能附加机卡绑定（或不能分离）的条款。

**5.3移动终端管理软件需求**

**5.3.1移动警务终端管理软件**

1) 定制173套移动警务终端管理软件及部署承载后台管控平台的相关服务器硬件、网络环境及系统软件环境。

2) 满足不少于173台移动警务终端集中管理的后台管控平台。

3) MDM技术支持。

① 能实现对特定终端远程下发APN运营商联网接入点；

② 实现后台查看设备定位坐标、日期时间与地图；

③ 可根据实际需求开启或关闭终端管控中的部分功能；

④ 实现终端消息提醒时，将系统提示及应用消息实时采集并上报至服务端，包括文字内容、应用名称、终端信息等；

⑤ 实现将MDM服务器采集过来的消息数据传递到对应用户生活系统；

⑥ 实现系统服务端API接口，可授权第三方应用读取用户信息、推送消息内容、终端信息等；

⑦ 符合广州公安移动警务安全规范要求。

4) MDM运维支持。

① 需积极响应服务软件运行过程的兼容问题；

② 需提供运维支撑人员协助进行业务操作；

③ 需提供7x24小时紧急处理支持与技术支持。

5) 后台管控平台的功能模块：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能模块** | **功能列表** | **功能细则** | **功能描述** |
| 1 | 人员组织管理 | 组织管理 | 人员组织结构创建、修改、删除、查询功能 | 可以根据用户的组织结构进行手工或者导入方式创建无限层级的组织结构数据，并提供修改、删除、查询功能 |
| 人员管理 | 人员上传 | 可以手工或者批量导入人员姓名、部门等信息 |
| 人员维护 | 人员的增、改、查、批量导入，绑定人员和IMSI信息。基于政务微信的人员架构进行部署，如果人员调动了，自动推送人员当前部门相关管理策略和应用，并删除之前部门应用 |
| 分组管理 | 对人员进行分组 | 除可根据组织机构的方式进行管理外，平台还可为根据管理要求对跨组织部门的人员创建分组，并可以对分组分配所有管理策略。 |
| 权限管理 | 为组织或者分组创建管理员 | 可以为任意一级组织或者分组设定管理员 |
| 管理员权限设置 | 可以为上述任一管理员进行管理权限分配 |
| 2 | 安装管理 | 注册管理 | 预注册 | 可在后台通过批量导入用户信息和终端IMEI、SIM卡IMSI等信息 |
| 自注册 | 终端使用者自行通过输入服务器地址、用户名（警员信息等）进行注册并且激活 |
| 管控安装 | 预安装 | 支持将管控软件内置于终端系统内 |
| 自安装 | 可输入网址进行下载与安装管控软件 |
| 激活管理 | 终端激活 | 设备安装客户端并插入SIM卡，通过扫描注册二维码即可完成注册激活 |
| 初始化策略执行生效 | 终端激活后自动生效用户归属的部门或者分组的管理策略，并自动安装被分配必须安装的软件 |
| 网络可用 | 安全客户端兼容与保活 | 支持安全客户端进程保活，同时确保管控系统开启情况下不影响网络的通畅性 |
| 禁止网络热点共享 | 禁止通过USB网络分享、蓝牙网络分享以及热点分享功能 |
| 升级管理 | 需支持平滑安装管控软件 | 预安装、自安装、激活及升级管控软件时，需保证数据不丢失，且升级后应用可正常使用 |
| 配合进行管控系统安装 | 确保每台移动设备可正常安装并激活使用，且不得影响其他应用的正常使用 |
| 3 | 设备管理 | 外设端口管控 | WiFi与移动数据连接 | WiFi与移动数据连接的功能远程开启/禁用 |
| 飞行模式管理 | 管理平台可以远程设置飞行模式的开启/关闭 |
| NFC连接管理 | 管理平台可以远程设置NFC功能的开启/关闭 |
| 蓝牙连接管理 | 管理平台可以远程设置蓝牙的开启/关闭 |
| USB、文件管理 | USB、文件管理功能开启/禁用 |
| 开发者调试模式管理 | 管理平台可以下发指令禁止/开启开发者调试模式 |
| 机卡绑定锁机策略管理 | SIM卡与绑定手机分开时锁机功能可设置开启/关闭 |
| 摄像头、麦克风 | 摄像头、麦克风功能开启/禁用 |
| 截屏、录屏功能 | 截图、录屏功能可开启或禁止 |
| 设备管控 | 禁止修改终端时间 | 禁止用户手工修改终端的系统时间 |
| 时间同步机制 | 终端以后台服务器时间为基准，自动同步较正终端时间 |
| 端到端管理 | 管理员可以通过手机对自己管理权限范围内的终端设备进行管理，包括锁定设备、寻找设备、盘点设备、设定设备可用等功能 |
| 远程协助 | 管理员通过管控平台对终端发起远程协助，终端接受许可后，管理员在管控PC上可以远程接管该终端安全工作系统的界面 |
| 蓝牙可配对名单 | 可配对名单内的蓝牙设备，终端允许连接，可配对名单外的蓝牙设备，终端禁止连接 |
| 文件管理 | 终端文件管理 | 支持单个或批量下发文档、图片、音频或视频等格式的文件。支持单个或批量删除文档、图片、音频或视频等格式的文件。 |
| 丢失管理 | 定位及轨迹管理 | 系统可强制开启用户端北斗定位功能，可获得基站定位，可以实时精准定位终端位置，并对轨迹进行记录，管理员通过管理平台可以查看轨迹信息，轨迹信息默认保存一周，可配置。 |
| 远程锁机 | 通过管理平台可以远程下发指令对终端进行锁机 |
| 终端丢失 | 终端发生丢失时支持擦除终端数据、格式化内置与外置存储 |
| 手机注销 | 支持注销手机管理，注销后手机结束管理状态，清空管理指令 |
| 终端解绑 | 支持解绑替换用户、替换安全卡、替换SIM卡等 |
| 4 | 应用管理 | 应用管理 | 应用准入名单 | 平台支持应用准入名单，支持增、删、改、查、导入操作，客户端仅允许准入名单中的应用可以下载安装并使用，禁止手机使用准入名单外的应用 |
| 应用推送名单 | 平台支持应用推送名单，支持增、删、改、查、导入操作，对终端上未安装的推送名单应用进行自动下载及后台静默安装 |
| 应用安装 | 平台支持对移动终端下发策略实现应用自动下载、并静默/强制安装 |
| 应用安装功能限制 | 当限制安装功能时，手机上所有的软件安装包均无法执行安装 |
| 应用卸载 | 手动卸载：用户可手动卸载不需要使用的应用；静默卸载：管理员可以通过管理平台下发策略，远程静默卸载终端上指定的应用 |
| 应用卸载功能限制 | 当限制卸载功能时，所安装的指定应用均无法卸载 |
| 应用更新 | 终端定时检测新应用发布信息，提醒用户新版本软件更新信息，并可自动下载、并静默/强制更新 |
| 应用商店后台功能 | 应用上传 | 应用上传可以指定管理员实施，上传时需提供应用相关信息，包括应用版本信息、应用名称、应用类型、应用介绍、应用图片信息。 |
| 应用取消分配 | 管理员取消应用分配后，终端上的应用商店中该应用不再展现 |
| 应用分类 | 对上传的介质进行分类，方便查找和管理，可根据需求自由分类 |
| 禁用/允许系统自带应用商店 | 禁止/允许使用系统自带应用商店 |
| 应用商店前端功能 | 应用商店基本功能 | 支持在设备上的应用商店客户端获取允许该设备/用户可安装列表；支持按名称查询；支持查看具体应用介绍 |
| 软件下载功能 | 保证客户端连接合法情况下，支持应用安装包断点续传。在下载失败后需要应提示用户重新下载 |
| 应用商城防卸载 | 产品支持客户端卸载保护机制，用户在界面上无法卸载客户端，管理员卸载客户端应用程序需要通过输入卸载密码或通过管理中心指令卸载。 |
| 应用下载失败恢复处理 | 系统支持当客户端应用下载失败后通过断点续传继续下载，直到下载完成 |
| 更新通知方式 | 支持开启/关闭通过应用商店管理端对移动设备进行更新通知 |
| 通知信息下发 | 支持后台对单台、批量终端下发提示信息或文本通知 |
| 5 | 安全管理 | 设备安全 | 全设备擦除 | 通过管理平台下发指令可以远程对终端进行全设备擦除，擦除后的终端恢复为出厂设置状态 |
| 密码远程设置或修改 | 通过管理平台可以远程下发指令对终端登陆密码进行设置或修改，终端接受指令后会被更新密码并锁屏要求重新输入密码验证 |
| 清除密码 | 通过管理平台可以远程下发指令对终端登陆密码进行清除，终端接受指令后锁屏密码被设置为指定 |
| 离线密码 | 客户端和后台使用同一套算法生成动态离线密码，以避免网络无法连接导致设备锁定后无法解锁。 |
| 机卡绑定 | 可对某台或批量终端的IMEI、SIM卡和加密卡进行绑定，一旦移动将被锁机 |
| 异常管理 | 当检测到终端被Root后，终端将进行锁机、擦除等等管理，且管理指令无论是在网或者离线状态下都会生效执行。 |
| 6 | 资产管理 | 硬件资产 | 终端厂商 | 后台管控平台可以查看终端的厂商名字 |
| 终端型号 | 后台管控平台可以查看终端的型号 |
| CPU型号 | 后台管控平台可以查看终端的CPU型号 |
| CPU使用率 | 后台管控平台可以查看终端的CPU使用率 |
| 运行内存容量 | 后台管控平台可以查看终端的运行内存容量 |
| 内部存储容量 | 后台管控平台可以查看终端的内部存储容量 |
| 内部存储使用率 | 后台管控平台可以查看终端的内部存储使用率 |
| 电池电量信息 | 后台管控平台可以查看终端的电池电量信息 |
| 序列号 | 后台管控平台可以查看终端的设备序列号IMEI |
| 软件资产 | 软件资产管理 | 后台管控平台可以查看终端的软件名称、包名、版本号、软件大小、是否系统应用、是否准入名单应用、安装时间、上报时间 |
| 操作系统版本 | 后台管控平台可以查看终端的操作系统版本号 |
| 状态管理 | 手机信息查询 | 后台管控平台可以查看终端的手机号码、用户名称、所属部门、手机状态、是否在线、是否Root、是否外出、是否失联、最后连接时间等信息 |
| 查看设备上各功能状态 | 后台管控平台可以查看终端被后台管理平台禁用/启用的功能及状态 |
| 资产报表与统计 | 后台管控平台可以查看导出终端状态、应用安装统计数 |
| 7 | 围栏管理 | 围栏管理 | 时间围栏 | 可配置时间围栏的管理动作，当手机到达设定的时间自动触发执行时间围栏配置的管理，（时区变化后时区矫正，自动更新，时区策略） |
| 地理围栏 | 可配置地理围栏的管理动作（围栏内或者围栏外），当手机在指定的地理位置时自动触发执行地理围栏配置的管理 |
| 8 | 强壮性  管理 | 强壮性  管理 | 管控软件防卸载 | 产品支持管控客户端卸载保护机制，用户无法卸载客户端。管理员卸载客户端应用程序需要通过输入卸载密码或通过管理中心指令卸载 |
| 防止恢复出厂（增强受控终端） | 恢复出厂设置后不进行注册无法使用 |
| 管控软件系统权限保活 | 系统清理内存模式下、低电量模式下、息屏后台进程清理情况下管控软件进程依然保活 |
| 能耗管理 | 在终端必要系统软件正常运行情况下，安装并激活终端管控app，平均每小时耗电增加不超过20毫安 |
| 终端管理 | 要求系统能够承载管理≥10000台设备，且能够根据实际需要进行线性扩容 |
| 系统响应 | 实时管控命令反馈：≤5秒 |
| 9 | 策略管理 | 策略管理 | 制定策略 | 通过管理平台可分组实现终端控制策略的指定，包括：管理策略创建、配置、修改、删除、按组分配 |
| 分发策略 | 管理策略实时推送、批量发送 |
| 对离线终端，在终端上线后自动发送相应策略 |
| 可制定终端本地策略，无论终端是否在线策略均可被调度生效 |
| 根据用户需要开关特定策略模块 | 可根据不同用户实际所需制定不同的策略开关，包括：机卡绑定开关、锁机开关 |
| 策略执行跟踪 | 在策略分配后，查看策略执行情况 |
| 查看策略分配任务执行列表（策略名称、执行人、执行时间） |
| 点击单行展示指令总数、未执行数、已执行数、取消数 |
| 手机执行列表明细查看、导出 |
| 取回当前所有被控设备状态值 | 后台管理平台可以查看终端的被管控状态值 |
| 10 | 报表管理 | 报表管理 | 手机报表 | 支持手机离线、ROOT、失联（包含失联时间配置小时展示）的查询及导出 |
| 限制状态报表 | 手机限制情况查询分析。展示当前手机蓝牙、摄像头、麦克风、WIFI、移动数据的限制情况 |
| 应用报表 | 汇总手机上应用的安装情况，按照应用的安装量降序展示，可查看应用的详细安装信息，包括应用名称、包名、版本名称、是否系统应用、手机ID、手机号码、用户名称、所属部门，支持报表导出功能 |
| 管理员日志报表 | 记录管理员的操作日志，支持查询和导出报表 |
| 客户端自更新统计 | 查询统计MDM客户端新版本的更新情况 |
| 已注册数--数据审计模块 | 统计当前管理范围内已注册手机数量 |
| 在线数--数据审计模块 | 统计当前管理范围内在线的手机数量 |
| 越狱数--数据审计模块 | 统计当前管理范围内被Root的手机数量 |
| 失联数--数据审计模块 | 统计当前管理范围内离线时间超过设置的失联时间的手机数量 |
| 日新增手机量统计图--数据审计模块 | 以折线图形式展示一周内管理范围内每日新注册手机情况 |
| 日指令发送量折线图--数据审计模块 | 以折线图形式展示一周内管理范围内管理员每日发送指令总数情况 |
| 设备失联监控--数据审计模块 | 实时显示管理范围内的失联手机记录 |
| 11 | 运维管理 | 响应要求 | 半小时内响应 | 需半小时内回复跟踪管理软件相关问题 |
| 7x24小时响应服务 | 7x24小时有负责工程师处理系统问题 |
| 3小时内解决 | 需3小时内解决管理软件问题 |

6）MDM运维相关责任

① 负责处理应用推送、锁机、定位找回等技术操作。

② 负责数据统计、数据报表导出与分析工作。

③ 负责系统对接、系统兼容、扩容升级等工作，保障MDM系统的高效稳定。

**（六）项目实施和服务要求**

**6.1供货及验收要求**

**6.1.1供货要求**

自合同签订后，在2024年9月1日前，乙方完成173个用户的移动警务通信服务套餐（含173个警务应用语音流量套餐及配套的173台双系统移动警务终端、173个移动警务安全智能薄膜卡）的供货与调试完毕及办妥携号转网业务（如有）。自合同签订后起一周内派1名开发工程师调试移动警务通信服务辅助软件及工具。另外多提供3台移动警务终端备用设备以及3张移动警务安全智能薄膜卡备用的供货。设备供货需同时做到以下要求：

1)提供安装时记录的加密卡串号、流量卡iccid号、移动警务终端串号，对共173台移动警务终端进行全面清点、梳理，形成详尽电子台账。换机不换号，确保业务连续性，补卡或者携号转网中断时间不超15分钟。携转实施及费用由中标方承担。同时制作173个牢固、可靠、耐用的标签（须采用刻字等方式载明加密卡登记人、流量卡号码、移动警务终端串号等基本信息，具体样式等与甲方商定并报甲方同意后实施），以确保长时间使用不脱落的牢固方式固定在每一台移动警务终端上，安装完毕后协助甲方将设备打标签、封箱、分派，确保173个语音流量套餐和配备的所有设备的正常运行。

2)乙方需要安排服务团队上门配合采购人处理终端发放相关管理工作，包括上门对5G/4G专网通信卡所有用户的实名认证（包含市局大院外单位）、证书写入安全智能薄膜卡、完成5G/4G上网卡与安全智能薄膜卡的贴合、MDM安装配置，确保终端能够正常使用。终端调试完毕，乙方需要安排服务团队分别配送终端到各用户所在单位（包括广州市公安局大院及市局大院外单位），配送的相关费用由乙方承担。

3)完成上述供货内容后，必须对广州市公安局移动警务的应用软件进行安装、测试与试运行。173个用户的移动警务通信服务的移动警务终端的应用软件进行安装、测试与试运行期间的服务与通信资费由乙方免费承担。待应用软件能够在项目提供的设备上正常运行与使用，方可进行项目设备供货验收。

**6.1.2供货验收要求及方式**

1)乙方完成所有的交货、安装调试结束，在货物数量、规格、质量、应用软件可正常使用及各项功能应用满足合同要求后，由甲方、乙方双方共同签字验收。甲方组成的验收小组按国家有关规定、规范进行验收，经检验货物、安装质量以及广州市公安局移动警务应用软件在使用上无任何问题，由甲方组成的验收小组签署验收报告。因货物质量问题发生争议时，由本地质量技术监督部门鉴定。货物符合质量技术标准的，鉴定费由甲方承担；否则鉴定费由乙方承担。

2)乙方若因非不可抗力因素无法在合同条款的供货期内按时供货，乙方逾期交付货物的，以逾期交货部分货款总额每日5‰的标准向甲方交纳违约金，累计不超过逾期交货部分货款总额的10 %；交货未能通过甲方验收超过30日历日，视为违约，甲方有权解除合同，在解除合同后乙方需在10个日历日内退回已收取的合同款项，并交纳合同总价10%的违约金。

3)所有货物在验收时必须完好无破损，数量、质量及指标不低于投标文件要求，验收时如发现所交付的设备有短缺、次品、损坏或其他不符合合同、招标文件、投标文件规定之情形者，甲方应作出详尽的现场记录，或由甲方和乙方双方签署备忘录。此现场记录或备忘录可用作补充、缺失和更换部件的有效证据。由此产生的有关费用由乙方承担。

4)如果合同设备运输和安装调试过程中因事故造成货物短缺、损坏，乙方应及时安排换货，以保证合同货物成功完整支付。换货的相关费用由乙方承担。

5)甲方有权单方面对乙方提供的设备进行检测。如货物质量达不到投标文件的要求，则拒绝收货，甲方与乙方因设备的质量问题而发生争议，由甲方单方面交质量监督检测单位按投标文件技术性能要求检测，如检测结果不符合投标文件要求，甲方有权单方面要求乙方在5个工作日内对全部已到货物进行更换。更换的货物必须完成规定检测过程并取得符合投标文件要求的检测合格报告。如乙方更换后货物仍无法按要求取得达到投标文件技术性能要求的检测合格报告，甲方有权单方面中止采购合同。所涉及的检测费、运输费及其他发生的相关费用及责任，除由甲方的人为原因而出现的，均由乙方负责，甲方有权追索乙方违约责任，如按照甲方要求对乙方所提供设备交质量监督检测单位检测后设备符合投标文件的要求，检测费用由甲方承担。

6)如果乙方所提供的设备被有关部门认定为违反国家有关行业安全和质量规定及违法侵权等，由此而引起的一切后果和责任均由乙方负全责。

7)若乙方提供的产品发生知识产权纠纷的，由乙方与原知识产权所有者协商解决，甲方不承担与之相关的任何经济和法律责任。

**6.2项目服务期起算办法**

乙方完成项目共173个用户的移动警务通信服务的设备供货后，由甲方组织供货验收（验收要求见用户需求“6.1.2供货验收要求及方式”），服务期自供货验收通过之日起开始计算3年。

**6.3项目服务的用户验收**

通过供货验收并且整体服务稳定运行满36个月后，甲方组织对项目进行用户验收，由甲方组织验收小组进行对供货验收后36个月的整体服务情况进行验收评审，通过验收后签署验收报告。

**6.4项目运维维护要求**

日常检测机制：在试运行期间，每天定时检测所有设备的运行状况，及时排除系统存在的隐患。

应急响应机制：实施24小时值班制度，在发生故障时要在第一时间内，运行维护人员快速给现场人员予以解答（工作日15分钟内到达现场），并在现场人员无法解决情况下，厂家维护人员两小时内赶到现场处置突发故障。

**6.5售后服务要求**

**6.5.1保修期内的售后服务**

1) 所有配套设备均须由乙方提供项目期内保修服务，保修费由乙方承担。

2) 在3年服务期内配套的所有主要设备（包括173个警务应用语音流量套餐及配套的173台双系统移动警务终端、173个移动警务安全智能薄膜卡）需提供三年的三包服务，手机终端需采购三年碎屏险；如故障属人为（以指定维修点提供的故障检测单作为依据），经甲方同意后，则按指定官方维修点的定价，经与甲方协商同意后进行维修。

因公安业务的特殊性，乙方需承诺承担额外因公安业务导致的人为故障维修费用。

3) 配套设备的配件的保修承诺如下：电池、充电器、数据线保修不少于一年，耳机保修不少于三个月。

4) 保修期内，乙方需组建独立运营运维团队支撑甲方工作，包含项目经理、技术负责人与支撑人员，包括运营支撑岗位1人、运维支撑岗位2人以及技术支撑岗位1人。

其中，项目经理要求满足以下条件：①2年或以上政务信息系统相关经验，②熟练掌握运维管理、质量管理和版本管理知识，并具备实际项目运维处理经验，③具备有效沟通能力和独立完成工作的能力，④具备优秀的文档编制能力、执行力、协调和组织能力，⑤具备较强的数据分析能力；同时，需满足以下条件中的至少一项：1、具有信息系统项目管理师证书；2、具有系统规划与管理师证书；3、具有通信专业技术人员资格证书；4、具有系统集成项目管理工程师证书；5、具有本科或以上学位。

技术负责人要求满足以下条件中至少一项：1、具有通信专业技术人员资格证书；2、具有网络工程师证书；3、具有本科或以上学位。

运维团队具体职责与能力要求如下：

① 运营支撑岗位1人

职责：

a)负责组织协调技术团队和运维团队保障项目的顺利上线、变更、运行；

b)针对全局移动警务使用情况，整理运营报告，分析存在问题，提出改进措施；

c)负责组织系统运行过程中问题的分析工作；

d)负责制定合理可行的、可追踪高效的运维计划与故障处理机制；

e)负责问题分析与人员分配、协调各相关方处理故障问题、编制运营运维报告；

f)制作项目进度网络图、工作流程图、业务流程图、宣传PPT等工作。

要求：

a) 3年以上政务信息系统相关经验；

b) 熟练掌握运维管理、质量管理和版本管理知识，并具备实际项目运维处理经验；

c) 具备较强的PPT制作、数据分析能力；

d) 具备有效沟通能力和独立完成工作的能力；

e) 具备优秀的文档编制能力、执行力、协调和组织能力；

f) 熟悉顶层设计、总体规划等方法论

② 运维支撑岗位2人

职责：

a) 负责运维报障、bug管理与问题跟踪；

b) 负责编写测试相关文档；

c) 负责执行项目测试，包括构建测试环境，设计和执行测试用例，缺陷跟踪和质量分析等；

d) 在项目中保持和项目经理、运营支撑人员的积极有效沟通，快速推动问题解决；

e) 负责测试各阶段的流程、功能点与测试风险；

要求：

a) 具备软件测试、系统测试等相关知识与工具；

b) 具备安卓、web、网络等日常运维与问题排查的能力；

c) 具备Linux、TCP/IP、HTTP网络协议相关知识；

d) 具备一定的自动化测试经验，有安卓应用测试经验；

③ 技术支撑岗位1人

职责：

a) 负责数据运维、自动化运维过程中的脚本编写；

b) 负责推动建设自动化测试体系，协助团队提升测试的质量和效率；

c) 负责结合运维问题特征，挖掘业务相关的测试需求；

d) 负责应用的故障预防与质量保证，统计、分析度量数据的工作；

e) 负责数据爬取与统计工作；

f) 负责投票程序、问卷程序、统计后台、跨网消息推送、消息获取程序等功能性程序。

要求：

a) 熟练掌握Node.js、Python、Java (Android)其中一到两种开发语言；

b) 熟悉MySQL、SQLite、MongoDB等数据库；

c) 熟悉Linux、TCP/IP、HTTP网络基本知识；

d) 具备前端（Android与Web）开发经验、爬虫开发经验优先；

e) 具备一定的自动化测试经验，对自动化测试有一定的理解；

5) 乙方应在工程完成后及时向甲方提交有关工程竣工资料文件，包括但不限于移动终端管理软件等。

6) 在维修期间乙方无法现场修复的，乙方应提供相同或优于当前设备的备机作为替代使用，直至故障设备修复完毕交回甲方。

7) 乙方定期向甲方汇总移动通信套餐的语音费及流量费每月使用情况，提供定期上门服务，对设备进行保养维修、故障处理，每半年提供一次上门培训服务。

8) 乙方需承诺对广州市公安局的现存各运营商终端提供服务支撑、跟踪服务（具体售后工作由对应服务商提供）

**6.5.2培训要求**

甲方参加培训的交通费及食宿费由甲方自行负责。

乙方至少必须满足本章要求的培训服务：

1）对本项目的甲方技术人员提供培训服务，每年不少于两次上门培训。

2）乙方必须为所有被培训人员提供培训用文字资料和讲义等相关用品。所有的资料必须是中文书写。

3）乙方需根据甲方的要求，制作彩色软页操作手册，并在服务期内定期更新内容，一年不少于2次。

合同价应将所有培训费用（含培训教材费）等费用包含在内。

培训地点：广州市。

培训人数：具体人数由甲乙双方确认。

根据本项目涉及的业务及技术，针对甲方技术人员需要掌握的该项目工程各服务组件的日常维护操作、障碍处理等技能，提供包括但不限于以下内容的培训：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **培训项目** | **培训内容** | **参与人员** | **培训目的** | **培训方式/时间** |
| 1 | 终端介绍 | 双系统安全终端使用说明介绍 | 部门领导、业务主管、技术主管 | 熟练两种终端具体使用注意事项及使用流程。 | 半天。上门集中授课和交流。 |
| 2 | 警务移动终端管理服务平台介绍 | 移动终端管理服务及配套警务APP应用功能讲解 | 部门领导、业务主管、技术主管 | 熟练移动警务终端的操作使用流程及详细功能。 | 半天。上门集中授课和交流。 |
| 3 | 日常维护 | 终端日常维护要点 | 业务主管、技术主管 | 了解终端日常维护要点。 | 半天。上门集中授课和交流。 |
| 4 | 障碍处理 | 障碍段落的判断及障碍申告操作 | 部门领导、业务主管、技术主管 | 了解如何判断障碍段落及怎样向公司申告。 | 半天。上门集中授课和交流 |

**6.5.3其他服务要求**

1）在合同期满后，乙方承诺免费做好各项交接工作。乙方须保证，本项目所有数据存储介质（包括硬盘、SD卡等）故障不回收。

2）本次项目的移动警务终端通信服务到期后，终端及薄膜卡的免费使用权限为永久，乙方需承诺根据甲方需求免费提供终端及安全智能薄膜卡给甲方使用。如甲方不需要继续使用，乙方承诺需协助终端、安全智能薄膜卡以及相关敏感信息进行销毁、回收。信息脱敏工作需由具备相关资质的企业承担，所涉及费用由乙方承担。

3）乙方完全遵守《中华人民共和国妇女权益保障法》中关于“劳动和社会保障权益”的有关要求。

**6.5.4** **服务评价**

服务评价是指对服务期内的服务质量、响应时间的评价，主要是针对有无按照招标文件、投标文件、合同规定的采购、维护和保修条款履行义务。评价时间范围是项目整体责任维护期内。

项目验收服务评价办法如下：

每期付款前，甲方对乙方服务进行服务评价。服务评价是指对服务期内的服务质量、响应时间的评价，主要是按照合同规定的条款履行义务的评价。评价时间范围是项目服务期内。服务评价总分为100分。

具体评价方法：由甲方进行服务评分，满分为100分。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务评价 | 评价细则 | 评分 |
| 1 | 故障响应评分（30分） | 乙方接到报障通知后须在1小时内给予响应。优（5分钟内）：26-30分；良（10分钟内）：21-25分；中（30分钟内）：16-20分；差（超过30分钟）：15分及以下。 |  |
| 2 | 故障处置评分（30分） | 乙方在24小时内解决网络故障。优（30分钟内）：26-30分；良（1小时内）：21-25分；中（2小时内）：16-20分；差：15分及以下。 |  |
| 3 | 协助处置评分（20分） | 外单位造成系统发生的任何异常故障和损坏的，乙方应积极协助处理故障。优（非常满意）：16-20分；良（满意）：11-15分；中（一般）：5-10分；差（不满意）：5分及以下。 |  |
| 4 | 运维服务评分（20分） | 乙方提供其他运维服务，如号码清单整理、费用预警等运维服务。优（非常满意）：16-20分；良（满意）：11-15分；中（一般）：5-10分；差（不满意）：5分及以下。 |  |
| 5 | 合计（100分） |  |  |
| 备注 |  |  |  |

挂钩办法为：

|  |  |
| --- | --- |
| 验收服务评价得分 | 所得款项计算方法 |
| 90分以上（含90分） | 全额支付 |
| 80分至90分（含80分） | 实付款=应付款×80% |
| 70分至80分（含70分） | 实付款=应付款×70% |
| 60分至70分（含60分） | 实付款=应付款×60% |
| 低于60分 | 实付款=0，并追究中标人相关责任。 |

**二、支付方式**

　　1.甲方与乙方签订合同后20个工作日内，按合同总价的5%以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式向甲方提交履约保证金。支持乙方以电子保函代替履约保证金，乙方可通过广东政府采购智慧云平台金融服务中心在线办理电子履约保函业务。若乙方没有违约行为，履约保证金在合同有效期满后15个工作日内由甲方无息退还乙方。甲方逾期退还履约保证金的，除应当退还履约保证金的本金外，还应当按中国人民银行授权的全国银行间同业拆借中心在逾期当月20日（遇节假日顺延）9时30分公布的贷款市场报价利率上浮20％后的利率支付超期资金占用费，但因乙方自身原因导致无法及时退还的除外。下列任何一种情况发生时，甲方有权不予退还履约保证金：（一）有明显证据证明乙方未履行本合同约定的；（二）乙方有明显过错致甲方造成损失的。

2.自合同签订后起5个日历日内，甲方办理合同总额30%的支付手续；

3.在2025年6月30日前，甲方办理合同总额50%的支付手续，在本次合同款支付前，甲方将按照招标文件要求组织对投标人第一个服务期（自服务期起算日起前6个月）进行服务评价，得分为90分（含）以上，甲方按合同进度款全额支付；得分为90分（不含）至80分（含），甲方按合同进度款的80％支付；得分为80分（不含）至70分（含），甲方按合同进度款的70％支付；得分为70分（不含）至60分（含），甲方按合同进度款的60％支付；得分为60分（不含）以下，视为本周期服务不及格，扣除乙方全额合同进度款，并追究乙方相关责任；

4.用户验收通过后，办理合同总额20%的支付手续，在本次合同款支付前，甲方将按照招标文件要求组织对乙方第二个服务期（自服务期起算日起第7个月至第36个月）进行服务评价，得分为90分（含）以上，甲方按合同进度款全额支付；得分为90分（不含）至80分（含），甲方按合同进度款的80％支付；得分为80分（不含）至70分（含），甲方按合同进度款的70％支付；得分为70分（不含）至60分（含），甲方按合同进度款的60％支付；得分为60分（不含）以下，视为本周期服务不及格，扣除乙方全额合同进度款，并追究投标人相关责任；

5.乙方须在甲方办理付款手续之前5个工作日内，提供等额的正式发票给甲方，以便甲方及时办理付款手续。

6.因财政资金拨款不到位而导致甲方逾期付款的，甲方不承担违约责任。甲方在前款规定的付款时间为向政府采购支付部门提出办理财政支付申请手续的时间（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为甲方已经按期支付。

**三、保密责任**

（一）甲方保密责任：

1.保密内容：项目内容。

2.涉密人员范围：项目组成员。

（二）乙方保密责任：

1.保密内容：与本合同相关的所有技术和业务内容、数据、图表、文字、计算过程、电子文件及言谈记录等。

2.涉密人员范围：项目组成员。

3.保密期限：永久。

4.泄密责任：乙方如有违反合同附件3《保密协议》所规定的行为造成泄密的，应向甲方支付合同总价10%的违约金，并赔偿由此产生的一切经济损失；泄密造成严重影响的，甲方有单方面解除合同。并可提请司法机关依法追究乙方及相关人员的刑事责任。

**四、合同变更**

本合同的变更必须由双方协商一致，并以书面形式确定。另一方应当在15个工作日内予以答复；逾期未予答复的，视为同意：

乙方就甲方委托服务内容、功能的扩大向甲方要求增加相应的服务费用，由乙方提出变更内容，甲方审核通过后，双方签定补充合同，并根据合同内容支付服务费用。

**五、后续开发成果的归属**

（一）在本合同有效期内，甲方利用乙方提交的技术服务工作成果所完成的新的技术成果，归甲方所有。

（二）在本合同有效期内，乙方利用甲方提供的技术数据和工作条件所完成的新的技术成果，归甲方所有。

**六、项目联系人**

双方确定，在本合同有效期内，甲方指定　为甲方项目联系人，乙方指定　为乙方项目联系人。项目联系人承担以下责任：

（一）作为甲乙双方沟通的主要接口和联系渠道；

（二）落实或回应对各种请求的处理结果；

（三）定期或不定期拟定维护进展报告及需要协调解决的问题报告。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，责任方应承担相应的责任。

**七、违约责任**

（一）甲方逾期付款，每逾期1天，支付所欠款项0.3‰的违约金，违约金累计不超过服务费总额的10％。但由于财政资金拨款不到位而导致甲方逾期付款的，甲方不承担违约责任，并且此情况不能成为乙方拒绝提供服务的理由。

（二）乙方若因非不可抗力因素无法在合同条款的供货期内按时供货，乙方逾期交付货物的，以逾期交货部分货款总额日5‰的标准向甲方交纳违约金，累计不超过逾期交货部分货款总额的10%；

交货未能通过甲方验收超过30日历日，视为违约，甲方有权解除合同，在解除合同后乙方需在10个日历日内退回已收取的合同款项，并交纳合同总价10%的违约金。

（三）乙方违反本合同规定，未能达到约定的服务标准，甲方书面提出整改通知，累计提出达3次，甲方有权单方面终止合同，由此造成甲方经济损失的，乙方应给予经济赔偿。

**八、不可抗力**

（一）由于不可预见、不可避免、不可克服等不可抗力的原因，一方不能履行合同义务的，应当在不可抗力发生之日起10天内以书面形式通知对方，证明不可抗力事件的存在。

（二）不可抗力事件发生后，甲方和乙方应当积极寻求以合理的方式履行本合同。如不可抗力无法消除，致使合同目的无法实现的，双方均有权解除合同，且均不互相索赔。

**九、争议解决方式**

（一）凡与本合同有关的一切争议，甲乙双方应首先通过友好协商解决；如经协商后仍不能达成协议时，双方同意采取以下第2种方式解决：

1.向广州仲裁委员会申请仲裁；

2.向有管辖权的法院提出诉讼。

（二）本合同的诉讼管辖地为甲方所在地有管辖权的法院。

（三）在仲裁或诉讼期间，除有争议部分的事项外，合同其他部分仍应继续履行。

**十、通知**

（一）本合同一方给对方的通知，应用书面形式送达合同中规定的对方地址。电传或传真要经对方书面确认，以电传形式的通知，从当地邮电局发出电报的第二天视为送达。

（二）通知以送到日期或通知书的生效日期为生效日期，两者中以晚的一个日期为准。

**十一、合同生效**

本合同经双方授权代表签字并加盖合同专用章或公章之日起生效，合同生效日期以最后一个签字日为准。

**十二、其他**

（一）本项目附件均是本合同不可分割的部分，解释的顺序除特别说明外，以文件生成时间在后的为准。

（二）在执行合同过程中，所有经甲乙双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分，其生效日期为双方签字盖章确认的日期。

（三）除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

（四）本合同一式10份，甲方执6份、乙方执4份，具有同等法律效力。

**十三、合同附件**

1、保密协议

（以下无正文）

甲方（盖章）: 广州市公安局： 乙方（盖章）：

地址：广州市越秀区起义路200号 地址：

法定代表人： 法定代表人：

委托代理人： 委托代理人：

电话： 电话：

传真： 传真：

开户银行： 开户银行：

账号： 账号：

签约时间： 签约时间：

签约地点：广州市

**附件一：**保 密 协 议

甲 方：XXXXXX

乙 方：XXXXXX

协议乙方为甲方实施《XXXXXXXX(项目名称)》，由于双方在开展上述业务合作的过程中需交换各类信息；双方在开展各自业务的同时，需妥善保护双方交换的信息；为此，甲方、乙方同意就协议一方（“甲方”）向另一方（“乙方”）提供的任何信息（“视为保密信息”）所应承担的保密义务签署协议如下：

**第一条 定义**

“保密信息”指在本协议下的项目讨论过程中，甲方和乙方之间所有往来的书面资料、电子文档资料及访谈记录等，以及其它与本项目相关的信息，都将被视为保密信息。

**第二条 保密原则**

乙方同意不使用由甲方向其公开的保密信息作为己用。乙方只可以把甲方的保密信息公开给乙方需要此保密信息完成本协议的项目或业务合作的雇员。乙方不得向其他雇员或任何第三方泄漏另一方的保密信息，除非有甲方的书面许可。乙方同意对来自甲方的保密信息采取与其相对应密级的保密要求进行保护。乙方同意对引起乙方注意的任何误用或盗用保密信息的行为书面通知甲方。乙方对一些不明是否属于保密信息范畴的相关信息，必须以书面形式向甲方征询。所有未明确的相关信息，必须先按保密信息要求保密。

**第三条 期限**

本协议应自双方法定代表人或其授权签字人签字及盖章之日起开始生效，直至甲方同意保密信息公开或成为公开信息时终止。乙方不得在协议期限内解除本协议。相关合同的终止不等于保密条款终止。

**第四条 归还和销毁**

根据本协议向乙方提供的保密信息在本保密协议终止或甲方提出书面要求时，乙方应根据甲方的要求，或迅速归还给甲方，或由乙方在本协议终止后当面（甲方）销毁所有接受的保密信息材料，对于电子信息，也必须有效销毁。所有保密信息销毁后，乙方必须向甲方出具已销毁所有保密信息的书面保证书。

另外，对乙方的所有参与成员，本协议的保密要求将长期有效，必须长期继续履行保守已知的保密信息不泄漏，除非甲方书面明确可公开的信息或甲方同意协议终止外。

**第五条 保证**

双方均应保证自己的雇员遵守此协议包括（但不限于）令雇员签订保密协议，对其进行相关的法律常识培训等。乙方应将参与本项目员工的有关资料（如身份证复印件、职称证明、项目经验等）给甲方，如需更换员工需事先征得甲方同意并提交相应的资料。

本协议权利和义务不得转让或委托。

**第六条 违约责任**

协议双方应遵照本协议履行保密义务，一方违反本协议给对方造成损失的，应赔偿对方因此而造成的所有损失，若乙方违反了本协议，触犯国家法律的将追究其刑事责任。同时，在广州市政府采购部门中将乙方列入黑名单，禁止今后参与广州市的政府采购活动。

**第七条 法律与仲裁**

本协议的合法性、解释和执行都遵照中华人民共和国颁布的法律。任何因本协议产生或与本协议有关的所有争议应提交广州仲裁委员会,根据其届时有效的仲裁规则进行仲裁，仲裁地点在广州市进行。仲裁裁决为终局裁决，对双方均有约束力。

**第八条 效力**

本保密协议与本项目的合作协议具有同等的法律效力，两个协议缺一不可。

本协议一式X份，甲方执X份，乙方执壹份，经双方签字加盖后生效。

|  |  |  |  |
| --- | --- | --- | --- |
| 甲方： | （客户单位名称）（盖章） | 乙方： | XXXXXX（盖章） |
| 签约代表： |  | 签约代表： |  |
| 地 址： | （客户地址） | 地 址： |  |
| 电 话： |  | 电 话： |  |
| 传 真： |  | 传 真： |  |
| 签约日期： | 二〇二年 月 日 | 签约日期： | 二〇二年 月 日 |