**附件1：**

**古镇公安分局2024-2027年度政务信息化项目（警务通项目）非“**★**”、“**▲**”的条款中参与评审条款汇总表**

**《技术和服务要求响应表》**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 采购文件规定的技术和服务要求 | 投标文件响应的具体内容 | 型号 | 是否偏离 | 证明文件所在位置 | 备注 |
| 1 | **一、日常巡检与维护**  1.具体租赁明细如下：   |  |  |  | | --- | --- | --- | | 设备/套餐名称 | 租赁数量 | 报价上限 | | 终端A及配套套餐和服务 | 95套 | 202元/月 | | 终端B及配套套餐和服务 | 90套 | 244元/月 |   以上租赁数量以招标人签订合同实际数量为准  按本项目要求按时完成月套餐服务、双系统终端、安全加密卡服务、MDM终端管控服务、终端安装服务、省市互联链路、终端维护服务等内容进行维护。  3.合同签订后30个日历日内需保质保量交付项目采购的各项内容；项目周期里，如中标终端机型停产，中标人需提供同等或更高性能的同品牌合规替代机型，差价由中标人承担；在分项合同所约定的服务时间和服务内容范围内，采购人预留未办理的警务通终端、套餐、安全加密服务、MDM终端安全管控服务等，采购人可随时办理；服务期内，中标人提供采购内容的免费维保及技术支持服务。  4.警务通终端接入公安移动信息网，中标人须自行提供公安移动信息网入网所需设备，包含但不仅限于交换机、路由器等设备，并于签订合同后30个日历日内顺利与中山市公安局古镇分局入网设备对接入网。  5.服务期内终端故障时，中标人或其委托维修单位须在采购人监督下开展维修工作。  具体维护内容：  （1）确保移动警务终端正常使用，链路状态稳定，与省厅移动警务安全认证正常连接，支撑移动警务应用正常使用。  （2）稳定的高带宽接入，APN 用户不需绕行运营商核心网，缩短逻辑路径，降低时延。  （3）MEC 本地部署，配置灵活，利于业务部署和调整。  （4）可通过无线网切片技术，实现客户的无线专网，确保数据安全性和保密性。  （5）接入白名单要求：将本项目警务通号码设为白名单，优先加入附近基站。  （6）针对采购人实际需求提供相应的网络优化保障服务，例如大型活动、重要会议、节日保障以及特殊区域与位置的网络信号加强与优化保障。  （7）MDM终端管控系统  1）基本维护服务，基本服务指为保证系统正常运行所需的预防性维护、日常维护支持、数据备份支持等工作。包括：①日常维护技术支持：对系统进行维护，监控应用软件运行情况，保证系统正常运行。②数据安全性管理技术支持：对系统的数据备份和恢复进行技术支持，以备在异常情况下尽快恢复系统。  2）①升级支持服务，版本升级技术支持：应用软件版本的升级支撑服务。②第三方软件升级：在采购人已经购买的第三方软件的升级服务的情况下，中标人应在第三方软件升级时进行相关的技术支持。③7\*24小时电话技术咨询服务。④技术资料支持。提供全面详实的系统技术资料，当系统或网络发生变化时在5个工作日内更新相关文档。  3）故障排除。工作日要求服务人员5分钟内响应，10分钟内开展故障排查，30分钟内定位问题，1小时内解决问题，如硬件故障要求2小时内提供备用硬件到达现场更换。非工作日要求10分钟内响应，30分钟内到达现场，2小时内解决问题，如硬件故障要求6小时内提供备用硬件到达现场更换。  （8）安全加密卡服务需求  1）功能需求，安全加密卡需经国家密码管理局安全审查，采用国产密码算法。可放置在一般的SIM 卡上再插入智能终端的卡槽中，可为智能终端提供身份认证和信息加密服务，提供的主要加密服务包括：  1.1.是用于存储个人数字身份证书和签名私钥，为移动警务终端提供数字签名、签名验证和数据加解密等密码服务。  1.2.是用于实现SM1 算法和密钥管理，为移动警务终端提供基于 SM1 算法的数据加解密服务。移动警务终端设备配备安全加密卡，安装安全客户端软件后，具备以下功能：  ①用户识别功能：安全加密卡提供基于PIN码的用户识别功能，合法用户可以设置和修改用户口令，非法用户无法通过口令验证，因而也无法使用移动应用功能；此外，PIN 码验证提供防暴力破解功能，连续错误输入口令次数超过设定次数将导致安全加密卡PIN 码被锁定。  ②信息安全存储功能：安全加密卡通过访问控制提供密钥等关键信息的安全存储，该信息的存储对访问进行了特殊标记；对称密钥信息加密存储，必须通过用户身份识别后才能进行读写。  ③密码学运算功能：安全加密卡主要提供的密码学运算有：随机数生成国密SM1算法、国密 SM2算法、SHA1杂凑算法、RSA1024算法等。 |  |  |  |  |  |
| 2 | 2）参数需求  ②支持标准SIM 卡、Micro SIM 卡和 Nano SIM 卡三种 SIM 卡类型。  ③支持国密算法高速加解密，可满足流媒体加密需求。  ④低功耗设计，满足手机的应用环境。  ⑤支持基于国密算法的移动应用分发，防止未授权的应用访问。  ⑥全面支持Android、鸿蒙等主流操作系统平台。  ⑦安全加密卡支持SM1、SM2、SM3、SM4 等国密算法。  ⑧安全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。  ⑨安全加密卡可实现SM2 算法和密钥管理，为移动终端提供基于 SM2 算法的数据加解密服务。⑪SIM 卡可与安全加密卡插在同一卡槽。  ⑫SM2 密钥对生成不少于 0.1s/对。  ⑬SM2 签名不少于 13 次/s。  ⑭SM2 验证不少于 12 次/s。  ⑮SM2 加密不少于 5Kbps。  ⑯SM2 解密不少于 6Kbps。  ⑰SM3 摘要不少于 19Kbps。  ⑱SM1 加解密不少于 13Kbps。  ⑲SM4 加解密不少于 10Mbps。  ⑳工作温度：-25℃到+85℃；存放温度：-40℃到+125℃。  3）认证需求：具备等保三级备案证明（提供证书复印件（或扫描件）并加盖厂商公章）；在安全水平的移动通信服务平台实现身份认证能力； |  |  |  |  |  |
| 3 | **二、省市互联链路维护：**  1.提供平台定期巡检、故障检查、故障诊断、数据整理、数据备份迁移、服务联调等工作；提供在线7\*24小时在线支持服务。  2.移动平台终端软件版本配合省厅平台定期升级服务，包括新终端适配、软件功能升级、应用测试和适配、平台功能迭代升级等服务。  3.按需求提供相应的移动警务终端服务、移动警务通信服务、流量套餐配置服务、MDM 终端安全管控服务、安装服务、运维服务，并提供相应的业务办理服务及保障。  4.中标人必须向采购人提供本项目采购的所有软件模块的安装、测试和维护服务的全部内容。  5.中标人须提供项目所有管理、实施、服务人员的社保证明给采购人审核后方可进场。  6.服务期内，中标人对提供的软硬件产品提供质量保证服务及产品免费技术支持售后服务。 |  |  |  |  |  |
| 4 | 四、设备清单  |  |  | | --- | --- | | 月套餐 | 警务通：  1.每月通话不少于700分钟、100条短信、30G互联网流量、30G移动警务专网流量(全局用户专网流量形成流量池，各用户从流量池中使用专网流量)。当月互联网流量、专网流量未用完则结转下个月使用。本项目内警务通手机号码互打免费。 | | 双系统移动终端 | 1.满足公安部《智能手机型移动警务终端第1部分:增强受控终端或多模式终端技术要求》（GA/T1466.1-2018）《智能手机型移动警务终端第2部分：安全监控组件技术规范》（GA/T1466.2-2018）要求。  2.性能要求：详见“终端设备清单”。  5.服务期内，本项目所租赁的软硬件中标人均需免费维保（维修时需免费提供同型号或同品牌符合要求更高型号维修备用机）。  6.根据采购人要求定制开机动画。  7.服务期满后终端自然报废，不回收。 | | 安全加密卡服务 | 1）功能需求，安全加密卡需经国家密码管理局安全审查，采用国产密码算法。可放置在一般的SIM 卡上再插入智能终端的卡槽中，可为智能终端提供身份认证和信息加密服务，提供的主要加密服务包括：  1.1.是用于存储个人数字身份证书和签名私钥，为移动警务终端提供数字签名、签名验证和数据加解密等密码服务。  1.2.是用于实现SM1 算法和密钥管理，为移动警务终端提供基于 SM1 算法的数据加解密服务。移动警务终端设备配备安全加密卡，安装安全客户端软件后，具备以下功能：  ①用户识别功能：安全加密卡提供基于PIN码的用户识别功能，合法用户可以设置和修改用户口令，非法用户无法通过口令验证，因而也无法使用移动应用功能；此外，PIN 码验证提供防暴力破解功能，连续错误输入口令次数超过设定次数将导致安全加密卡PIN 码被锁定。  ②信息安全存储功能：安全加密卡通过访问控制提供密钥等关键信息的安全存储，该信息的存储对访问进行了特殊标记；对称密钥信息加密存储，必须通过用户身份识别后才能进行读写。  ③密码学运算功能：安全加密卡主要提供的密码学运算有：随机数生成国密SM1算法、国密 SM2算法、SHA1杂凑算法、RSA1024算法等。 | | MDM终端安全管控服务 | 1.开放平台API功能：提供管控能力开放 API，方便与统一业务平台和安全接入平台系统进行对接集成。还可以对界面进行定制化。  3.大屏显示：支持在系统首页大屏显示系统关键数据，包括：设备状态、用户信息、系统状态监控、设备状态、设备违规情况、策略执行情况、应用安装情况等关键数据显示。  4.在线帮助：管理平台支持在线帮助的功能，在每个页面上点击右上角的问号，即可在浏览器新的 Tab页打开当前所在页面的帮助信息。帮助信息包括每个功能页面的菜单导航操作、功能说明、FAQ、常用名词解释等信息。  5.管理员分级权限细分至操作：管理平台提供的权限模板可以将权限分配至每个模块下面对应的操作，实现更细粒度的控制。同时，管理员还可以选择不同的权限模板快速创建下级管理员。  6.移动控制台：提供管理平台的移动 APP，支持双因子验证、自动登录和IP锁定功能。在移动管理控制台可进行系统监控和部分轻量操作。  7.二维码激活：支持通过二维码下载客户端，通过扫描二维码激活设备，支持在用户列表预览/下载激活二维码，提高激活工作效率。  8.用户扩展字段：管理员可以给用户添加扩展字段，用于保存用户的扩展信息如警号，最多五个字段。  9.用户标签：支持静态标签和动态标签，可根据删选条件灵活设置标签。  10.必装应用设置：下发或更新警务应用时，提供多种灵活设置，可以设置应用必装或按需安装，支持静默安装、按时安装。并可统计用户应用安装情况。  11.安全容器：提供企业应用安全容器，支持将企业应用推送到安全容器，支持应用数据加解密功能，支持一键清除容器应用产生的数据，支持对容器应用的内部数据复制、剪切、粘贴功能控制，支持启动/禁用容器应用、支持是否允许使用相机、麦克风、地理位置、读取短信、联系人、通话记录、手机号码、发送短信、媒体库、蓝牙、拨打电话、数据共享和打印功能。  12.移动杀毒：提供企业杀毒客户端，支持配置自动扫描和处理危险的应用程序，手动扫描、升级病毒库，支持记录设备的所有杀毒记录，包括扫描时间、扫描应用数量、危险应用数量。  13.安全浏览器：提供安全浏览器功能，支持设置网址黑白名单，设置书签，上传网址访问记录功能。  14.远程协助：支持远程协助功能，当警务终端用户出现问题时，可在管理后台远程协助显示终端界面，快速解决问题，提高工作效率。  15.时间/地理WL：支持通过时间或地理纬度实现WL功能，支持在WL内连续锁屏、配置移动数据WF、禁用摄像头、禁用蓝牙、相机安全提示、安全提示、通话白名单。  16.机卡绑定：可设置机卡绑定策略，防止用户私自更换 SIM 卡。  17.报表：强大的报表功能，支持提供设备激活记录、资产报表、设备已安装应用报表、设备淘汰报表、设备违规处理报表、设备杀毒报表、UEM 客户端统计报表、通话记录报表、短信记录报表、数据流量报表、用户详情报表、应用详情报表、应用安装统计报表、应用黑白名单报表、合规策略报表、内容报表。并支持导出为 excel 或 pdf 格式，支持报表订阅，租赁服务期内免费维保服务，满足公安部、广东省公安厅对终端管控要求。 | | 终端安装服务 | 移动终端安装、调试（刷Rom、制作加密卡、设置拨号帐号、APP程序等）。 | | 省市互联链路 | 中标人所提供终端应满足以下链路要求：  1.移动警务系统终端到中山市局移动警务系统（VPN无线连接）3Gb带宽链路。  2.中山市局移动警务系统到广东省公安厅身份认证及安全接入3Gb带宽链路。  3.中山市局移动警务系统到中山本地视频专网的3Gb带宽链路。 | | 终端维护服务 | 1.提供平台定期巡检、故障检查、故障诊断、数据整理、数据备份迁移、服务联调等工作； 提供在线7\*24小时在线支持服务。  2.移动平台终端软件版本配合省厅平台定期升级服务，包括新终端适配、软件功能升级、应用测试和适配、平台功能迭代升级等服务。 | |  |  |  |  |  |
| 5 | 五、终端设备清单1.终端A参数  | **分类** | **分项** | **技术参数** | | --- | --- | --- | | 通用  配置  要求 | 基本需求 | 3.终端均需含原装充电器、充电线。 | | 操作系统 | 1.安卓 Android10.0 及以上或国产操作系统； | | 网络支持 | 1.支持标准 SIM 卡（15\*25mm）、Micro SIM 卡（15\*12mm）、Nano SIM（12.3\*8.8mm）中的一种； | | 传感器 | 1.支持RL识别；  2.具备 NFC 功能。 | | 摄像头 | 1.后置摄像头：≥5000万像素超光变摄像头(OIS光学防抖)，≥1200万像素超广角摄像头，≥1200万像素长焦摄像头（OIS光学防抖），支持自动对焦；  2.前置摄像头： ≥1300万像素超广角摄像头；  3.配置 LED 闪光灯，支持手电筒模式。 | | 传输功能 | 1.WLAN 协议 802.11 a/b/g/n/ac/ax,2x2z；  2.WLAN 频率 2.4GHz 和 5GHz；  3.支持 WLAN 直连；  4.支持不低于 Bluetooth5.2 协议；  5.支持 USB3.1 GEN1 及以上高速传输标准及充电功能和 OTG 功能。 | | 防护能力 | 持在GB/T 4208-2017（国内）标准下达到 IP68级防尘抗水能力。 | | 其它 | 1.工作系统和互联网系统能手动任意切换，支持指纹切换、快捷按钮切换；  2.工作系统应具备语音电话白名单或者等同功能；  4.终端可按需求出厂预制主流警务软件及APN 参数。 | | 性能  要求 | 屏幕性能 | 1.尺寸应为≥6.6 英寸；  2.色彩应为≥10.7亿色， P3 广色域；  3.屏幕类型：OLED 显示屏；  5.多点触控触摸屏，最多支持10点触控。 | | | | | 电池性能 | 1.使用锂聚合物电池；  2.电池容量≥4650mA，支持不低于66W快充。 | | |  |  |  |  |  |
| 6 | 2.终端B参数  | **分类** | **分项** | **技术参数** | | --- | --- | --- | | 通用  配置  要求 | 基本需求 | 3.终端均需含原装充电器、充电线。 | | 操作系统 | 1.安卓 Android10.0 及以上或国产操作系统； | | 网络支持 | 1.支持标准 SIM 卡（15\*25mm）、Micro SIM 卡（15\*12mm）、Nano SIM（12.3\*8.8mm）中的一种； | | 传感器 | 1.支持RL识别；  2.具备 NFC 功能。 | | 摄像头 | 1.后置摄像头：≥5000万像素超光变摄像头(OIS光学防抖)，≥1200万像素超广角摄像头，≥4800万像素长焦摄像头（OIS光学防抖），支持自动对焦；  2.前置摄像头： ≥1300万像素超广角摄像头；  3.配置 LED 闪光灯，支持手电筒模式。 | | 传输功能 | 1.WLAN 协议 802.11 a/b/g/n/ac/ax,2x2z；  2.WLAN 频率 2.4GHz 和 5GHz；  3.支持 WLAN 直连；  4.支持不低于 Bluetooth5.2 协议；  5.支持 USB3.1 GEN1 及以上高速传输标准及充电功能和 OTG 功能。 | | 防护能力 | 支持在GB/T 4208-2017（国内）标准下达到 IP68 级防尘抗水能力。 | | 其它 | 1.工作系统和互联网系统能手动任意切换，支持指纹切换、快捷按钮切换；  2.工作系统应具备语音电话白名单或者等同功能；  3.工作系统可支持对接主流警务通应用软件，免费开放接口，并能提供相应的技术支撑；  4.双系统终端可按照需求出厂预制主流警务软件及APN 参数。 | | 性能  要求 | 屏幕性能 | 1.尺寸应为≥6.8英寸；  2.色彩应为≥10.7亿色， P3 广色域；  3.屏幕类型：OLED 显示屏；  5.多点触控触摸屏，最多支持 10 点触控。 | | | | | | 电池性能 | 1.使用锂聚合物电池；  2.电池容量≥5000mA，支持不低于66W快充。 | |  |  |  |  |  |
| 7 | **六、考核办法**  （一）服务质量考核要求  由采购人成立质量考核小组，负责对中标人服务质量进行考核评分。采购人根据《中山市公安局古镇分局运维服务工作服务考核表》每月对中标人服务质量进行评价，每月的运维考核结果累计至下一期支付金额中扣罚。  （二）项目考核扣罚金计算方式  考核得分与结算挂钩，中标人每月都须接受采购人的考核，采购人以书面的形式告知中标人考核结果，每月考核如有扣罚的则需扣除当月服务费（中标金额/36个月）相应金额。按4个档次设置扣罚款项，具体如下：  （1）得分≥90分，无需扣罚；  （2）90＞得分≥80，扣罚当月服务费的10%；  （3）80＞得分≥70，扣罚当月服务费的20%；  （4）70＞得分，扣罚当月服务费的40%。  （三）违规违规红线考核要求  运维服务过程中，发生下列表格所述安全事件，造成重大后果的，采购人有权单方面解除合同，中标人应赔偿由此给采购人带来的损失。   |  |  | | --- | --- | | **考核类型** | **考核说明** | | 信息安全 | 由于运维服务团队人员失误造成业务系统出现数据丢失、  篡改等情况。 | | 网络安全 | 因运维团队自身失误导致发生重大网络事件，不可抗力因素除外。 | | 信息泄露 | 运维服务团队私自将公共数据、个人数据、政务数据等泄露或进行市场销售。 | | 群众信访 | 由于运维服务不到位，导致出现群众信访事件或聚众扰乱社会事件的。 | | 安全生产 | 特种工作人员未持有电工证、高空作安全员证书等专业资质，进行相关作业，造成安全生产事件的。 |   **（四）中山市公安局古镇分局运维服务工作服务考核表**  此表仅供参考，采购人在项目实施过程中可结合实际业务情况进行动态调整。可根据该表增加个性化考核指标，最终解释由采购人所有。   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **序号** | **考核**  **类别** | **考核项目** | **考核内容** | **扣分** | | 1 | 服务人员考核 | 人员岗位设置 | 符合要求实际驻场人数/合同要求人数，不满足要求人数，每发现一人次扣4分； |  | | 2 | 人员稳定性 | 服务人员在服务期间未经采购人许可出现更换，每发现一人次扣4分； |  | | 3 | 人员工作满意度 | 客户投诉每次扣4分，书面警告每次扣6分； |  | | 4 | 人员业务水平 | 考核工程师对业务的熟悉程度、相关知识掌握程度、运维项目保密工作等的考核。出现误操作事件每人次扣4分； |  | | 5 | 服务提供 | 网络接入 | 按合同要求，按时完成网络接入.每逾期一天，扣1分； |  | | 6 | 终端及配套 | 按合同要求提供终端、安全卡、终端管控服务，每少一项，每台每天扣0.3分； |  | | 7 | 违规业务 | 违规业务 | 对警务通用户推销办理宽带、有线电视等私人服务的，每发现一次扣1分；未及时解除个人宽带、有线电视绑定的，每逾期一天扣0.5分； |  | | 8 | 日常维护 | 巡检和应急支持 | 按要求完成日常运维任务，未按时进行巡检的，扣0.5分/次；未按要求响应支持应急和处理事件的，扣1分/次； |  | | 9 | 报告提交情况 | 按要求准时提交相关日报、月报、周报、季度报告、重大故障报告等相关报告，未按要求准时提交一次扣1分； |  | | 10 | 软硬件升级 | 软硬件升级前没有事先向采购人申请或沟通而造成不良影响的，扣1分/次；未按照采购人要求进行升级的，扣2分/次，造成不良影响的，扣3分/次。 |  | | 11 | 故障处理 | 出现故障后没按故障正确的处理流程操作导致重大损失和造成恶劣影响的，扣15分/次； |  | | 12 | 功能变更管理 | 未经管理方私自进行功能变更的，扣2分/次，未按时按质完成功能变更的，扣2分/次； |  | | 13 | 安全管理 | 违反安全管理制度，人为造成严重、重大故障的，扣15分/次； |  | | 14 | 响应型服务质量 | 事件响应时间达标率 | 达标率低于70%（扣6分）；低于80%（扣4分）；低于90%（扣2分）；低于100%（扣1分）； |  | | 15 | 事件处理时间达标率 | 达标率低于70%（扣6分）；低于80%（扣4分）；低于90%（扣2分）；低于100%（扣1分）； |  | | 16 | 事件完成率（已经完成的事件数/事件总数） | 达标率低于70%（扣6分）；低于80%（扣4分）；低于90%（扣2分）；低于100%（扣1分）； |  | | 17 | 备件服务 | 备件服务 | 在接到采购人需求无法在短时间内对设备完成修复的，应马上提供备件更换，超出采购人规定时间到达现场更换备件的扣1分/次； |  | | 18 | 因中标人没有按时更换备件造成重大事故的，扣15分/次； |  | | 19 | 抢修服务 | 抢修服务 | 在接到采购人抢修需求时，应在规定时间到达现场进行抢修，每超出30分钟到达现场，扣0.5分。 |  | |  | 总分 | | |  | |  |  |  |  |  |
| 8 | 七、保密要求 1.为切实加强大数据平台各项应用的安全使用和管理，确保国家秘密和警务工作秘密的绝对安全，严防出现因越权访问、违规操作等造成公安信息泄露、侵犯公民隐私的行为发生，系统用户必须严格落实公安信息共享查询应用“七不准”管理规定，并承诺做到：  （1）严格遵守国家保密法律、法规和有关规章制度，履行保密义务，保守党和国家的秘密、保守公安工作秘密。  （2）不将应用系统授权数字证书或账号转借他人使用。  （3）不违规申报和审批系统授权用户。  （4)不非法扫描、入侵系统，扰乱系统正常运行。  （5）不公开宣传、与无关人员谈论应用系统及其相关内容。  （6）不泄露、传播或出售通过应用系统获取的信息。  （7）不对应用系统应用违规行为隐瞒不报、包庇袒护。  （8）非因工作原因，不使用应用系统获取的各类信息。  2.应遵守采购人各项规章制度、工作流程和安全保密规定，接受采购人日常工作管理，做好安全检查与防范工作。驻场人员应按照采购人要求签署保密协议，承担安全保密责任和义务，并通过人防和技防手段确保运维过程中产生的各类交易信息数据安全保密。  3.中标人对采购人所提供的所有资料以及在合同签订、履行过程中所接触到的采购人及其关联公司的商业秘密、技术资料信息等资料和信息（统称“保密资料”）负有保密义务。未经采购人书面许可，中标人不得向任何第三方披露，不得将保密资料的部分或全部用于本合同约定事项以外的其他用途。中标人有义务对保密资料采取不低于对其本身商业秘密所采取的保护手段予以保护。中标人可仅为合同目的向其内部有知悉保密资料必要的工作人员披露保密资料，但同时须指示其工作人员遵守本条规定的保密及不披露义务。  4.中标人仅可以为履行合同之目的对保密资料进行复制。中标人不得以任何方式（如软硬盘、图纸、彩样、照片、菲林、光盘等）留存保密资料。中标人应当在完成本项目任务或本合同终止或解除时将保密资料原件全部返还采购人，并销毁所有复制件。中标人应当妥善保管保密资料，并对保密资料在中标人服务期间发生的被盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成采购人损失的，中标人应负责赔偿。  5.当出现下述情况时，本条对保密资料的限制不适用。当保密资料：  （1）并非中标人的过错而已经进入公有领域的。  （2）已通过该方的有关记录证明是由中标人独立开发的。  （3）由中标人从没有违反对采购人的保密义务的人合法取得的。  （4）法律要求中标人披露的，但中标人应在合理的时间提前通知采购人，使其得以采取其认为必要的保护措施。  6.如中标人违反合同关于保密的约定，中标人应赔偿因此而给采购人造成的一切损失。  7.保密条款自保密资料提供或披露之日起至永久有效。 |  |  |  |  |  |

**注：1.此表仅作为汇总参与评审的8项非“★”、“▲”的条款，按量化指标，每无偏离或正偏离1项得1分，满分8分；其余条款请投标人在制作投标文件中自行补充到《技术和服务要求响应表》中。**

**2.本表中“采购文件规定的技术和服务要求”的填写若与招标文件第二章“采购需求”中的表述不一致，以招标文件第二章“采购需求”中的表述为准。**