**招标公告附件2：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 | 标的名称 | 参数性质 | 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 |  |  | **三、日常巡检与维护**  **（一）具体方案**  1.本项目具体租赁明细如下：   |  |  | | --- | --- | | 设备/套餐名称 | 租赁数量 | | 终端A及配套套餐和服务 | 105套 | | 终端B及配套套餐和服务 | 65套 | | 合计 | 170套 |   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、MDM终端管控服务、省市互联链路、安装服务、驻点运维服务、配套交换机等内容进行维护。  2.自合同生效后30个自然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；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.服务期内终端发生故障时，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。 |  |  |  |  |  |
| 2 |  |  | （二）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：将本项目涉及的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  7.1.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。  7.2.①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。  7.3.故障排除。工作日要求驻点人员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小时内将问题解决，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，硬件故障要求6小时内更换新备件解决问题。 |  |  |  |  |  |
| 3 |  |  | 8.安全加密卡服务需求  8.1.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：  8.1.1.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。  8.1.2.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：  8.1.2.1.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。  8.1.2.2.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。  8.1.2.3.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。  8.2.参数需求  8.2.2.支持标准SIM 卡、Micro SIM 卡和 Nano SIM 卡三种 SIM 卡类型。  8.2.3.支持国密算法高速加解密，可满足流媒体加密需求。  8.2.4.低功耗设计，满足手机的应用环境。  8.2.5.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。  8.2.6.全面支持Android、鸿蒙等主流操作系统平台。  8.2.7.安全加密卡支持SM1、SM2、SM3、SM4 等国密算法。  8.2.8.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。  8.2.9.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。  8.2.11. SIM 卡可与安全加密卡插在同一卡槽。  8.2.12. SM2 密钥对生成不少于 0.1s/对。  8.2.13. SM2 签名不少于 13 次/s。  8.2.14. SM2 验证不少于 12 次/s。  8.2.15. SM2 加密不少于 5Kbps。  8.2.16. SM2 解密不少于 6Kbps。  8.2.17. SM3 摘要不少于 19Kbps。  8.2.18. SM1 加解密不少于 13Kbps。  8.2.19. SM4 加解密不少于 10Mbps。  8.2.20.工作温度：-25℃到+85℃；存放温度：-40℃到+125℃。  8.2.3认证需求，安全加密卡应具备与达到等级保护（三级）安全水平的移动通信服务平台实现身份认证能力； |  |  |  |  |  |
| 4 |  |  | 六、现场技术支持  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、驻点人员的社保证明或与其签订的劳动合同或服务协议等资料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。 |  |  |  |  |  |
| 5 |  |  | **八、设备清单**   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **序号** | **服务名称** | **具体内容** | **单位** | **数量** | **服务时间（月）** | | 1 | 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。 | 套 | 170 | 36 | | 2 | 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。 | 台 | 170 | 36 | | 3 | 安全加密卡服务 | 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主要有：随机数生成国密SM1 算法、国密 SM2 算法、SHA1 杂凑算法、RSA1024 算法等，其余要求详见“安全加密卡服务需求”。 | 张 | 170 | 36 | | 4 | 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。 | 套 | 170 | 36 | | 5 | 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）。 | 个 | 170 | 36 | | 6 | 省市互联链路 | 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1条。  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1条。  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1条。 | 条 | 3 | 36 | | 7 | 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。 | 项 | 1 | 36 | |  |  |  |  |  |
| 6 |  |  | **九、终端设备清单**  **（一）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。 | | |  |  |  |  |  |
| 7 |  |  | **（二）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。 | |  |  |  |  |  |
| 8 |  |  | **十、人员管理要求**  2.项目经理资质要求：项目经理需具有5年以上的资深信息化运维服务管理经验，并熟悉同类的信息系统。具有信息系统项目管理师等与项目相关证书者优先。  3.运维服务团队人员应满足以下要求：  3.1.具备良好的沟通协调能力；  3.2.熟悉掌握常用办公软件的使用；  3.3.熟悉操作系统及软硬件的安装诊断和维护；  3.4.熟悉服务器及主流数据库（Oracle、SQL等）的安装及配置维护；  3.5.遵守采购人的工作纪律，服从采购人的工作安排；  3.6.运维人员必须经双方资质审核合格后，才可上岗工作；  3.7.运维人员必须签订保密协议，不得泄露与项目、采购人相关内容。  3.9.若实际运维人员不符合工作要求，采购人有权要求更换；若运维人员有变更，需提前1个月书面通知采购人，经采购人审核同意后方可更换。  3.10.驻场运维人员的办公环境、场地、桌椅由采购人提供，其余办公所用设备及资料，如办公电脑、交通工具等由中标人自行承担。  3.11.运维人员需自备台式电脑（本条所称的电脑主要指：主机、显示器、打印机、以及所有的电脑网络产品和附属设备，各类应用软件等，并配备安全机箱。）中标人需提供运维监控软件，该软件需具备对运维人员在公安网进行运维操作时的日志进行记录与分析的功能，并按采购人网络信息安全和业务设备管理的要求进行管理，当驻点人员调岗或离职时需移交个人电脑中与本项目相关的全部资料，未经允许不得对外透露因运维过程知悉的包括但不限于代码、业务、信息等。  4.本项目合同生效后，为保证运维人员工作顺利开展，构建有效激励约束机制，促进运维人员遵守工作纪律、提升技术水平、保证工作质量、积极开展工作，需制定运维团队管理办法，具体包括：  4.1.制定考核机制，依托考核手段，提高运维人员工作积极性、规范化和计划性以及技术水平；  4.2.运维人员必须遵守采购人的各项规章制度，保持良好的工作形象和工作态度，做好日常巡检和故障处理等工作；  4.3.由中标人为运维人员配备运维所需设备；  4.4.采购人针对运维人员的巡检情况、故障解决能力、项目的稳定性等综合情况打分，纳入到考核；  4.5.若中标人更换技术服务团队人员，必须经过采购人审核同意；  4.6.运维人员接到故障任务，必须及时作出响应，并在规定时间内排除故障（远程或现场），同时提交处理报告；  4.7.运维人员被临时抽调进行其他工作时，需经过相关负责人审批后方可离岗。 |  |  |  |  |  |
| 9 |  |  | **十一、服务形式**  **1.驻场服务**  按照项目采购需求规定提供驻场服务，按质按量按时提供日常巡检、疑难解答、故障定位、故障排除、功能调整等服务。为完成采购人布置的任务，中标人应视情况安排项目成员驻场加班。  **2.远程支持**  中标人通过电话、QQ、电子邮件、传真、远程协助等方式为采购人提供每周7\*24小时电话技术支持服务、7\*24小时微信技术咨询服务，协助采购人进行故障定位和故障排除。采购人的电话享有高度优先级，得到优先处理，直到设备、系统恢复正常运行。  **3.紧急现场服务**  每天（含重要节假日）24小时内，中标人接到采购人的维护需求后，属于维护服务范围的，应立即指派具备相应能力的技术工程师在约定时间内到达故障现场，处理在服务期内出现的重大故障或重大事件。  **4.故障处理服务**  采购人在使用软件系统中遇到疑难问题或系统出现不稳定情况，中标人需提供7\*24小时故障处理服务，并在规定时间内进行故障排除，及时定位故障并进行故障处理，减少或避免由于系统故障导致的损失。  **5.值守服务**  重要节假日、重大活动（重大会议、重大活动、敏感时间段）期间，若采购人提出项目24小时值守需求，中标人需按采购人需求作出响应。  **十二、培训服务要求**  在运维期间，中标人为采购人提供不少于1次培训，若采购人提出培训需求，中标人需及时作出响应，并安排讲师进行培训。为了达到良好的培训效果，中标人需提供相关培训教材及培训用具，应在培训前制定好详细的培训计划，罗列培训时间、地点、硬件和软件环境以及授课教师资质，为每个受训者提供一套培训材料，包括练习题、讲义、实验题等。  根据采购人实际需要，在采购人指定范围内提供针对本项目信息系统系统架构设计、业务数据流、模块与模块之间关系，系统数据库结构关系和对数据库、应用服务器监控、系统调优专业课程及业务系统操作等的相关培训。在培训后制作问卷向采购人问询满意度，若采购人有需求，则需改进授课的方式，争取让采购人满意。  **十三、维护工作执行办法**  中标人需按服务要求定期进行日常巡检，采购人不定期进行抽检；中标人需每季度进行全面巡检，并提交照片和巡检报告，每周、每月、每季度定期向采购人提交周报、月报、季度报，作为考核和请款依据。  1.中标人需按合同约定的要求开展日常巡检和运维服务工作，如发现质量问题将追究中标人相应责任并根据考核结果扣除相应运维费。  2.对涉及采购人的全部信息以及其他信息负有保密义务，未经采购人书面许可，中标人不得以任何理由和形式私自使用及向外泄露。  3.中标人需了解采购人的使用情况，针对近期发生的故障分析产生的原因，培训采购人工作人员正确使用设备。  4.中标人需安排专人进行资料管理。所有采购人的资料，每次在巡检中都应检查，并及时更新，使在册资料与实际情况完全保持一致。  5.维护过程中，需要维修的故障在维修前需要向采购人进行书面确认，待维护完毕后同样需采购人书面确认后方可离场。  6.中标人需配合采购人完成本项目范围内系统的网络安全等级保护测评工作与第三方软件测评工作。  7.中标人需配合采购人完成项目审计工作，包括但不限于审计材料的收集与整理。  8.驻点综合管理团队需记录事件发生地点、设备名称、时间、事件现象等相关信息，形成运维事件处理登记表，综合管理团队根据事件现象判断运维事件类型，事件类型包括网络事件、硬件事件、软件事件，并根据判断结果指派工作人员，同时根据运维管理规定录入信息化运维事件工单，受指派工作人员到达事件现场，评估事件产生原因、影响力、重要性、紧迫性，决定是否需要启动应急预案，若需启动应急预案，则上报应急领导小组并执行应急预案管理流程，运维过程中判断中标人是否能独立完成运维，若不能，则考虑将服务外包，并执行服务外包管理流程，输出运维事件处理记录表，事件处理过程中判断是否需要变更运维，若需变更，则按照运维变更处理流程开展工作，最后当运维变更需求处理结束确认无误后，管理员关闭工单，并将此次运维事件的处理方法录入运维知识库以备日后参考，流程结束。  img |  |  |  |  |  |
| 10 |  |  | **十四、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。  **十五、安全管理要求**  1.中标人是业务安全生产管理主体，对业务安全生产管理工作负全责。  2.中标人负责日常安全生产管理，采购人只负责对中标人进行考核和必要的监督检查。  3.按“谁聘用、谁负责”原则，中标人负责从业人员安全教育培训工作。  4.劳动保护用品发放由从业人员劳动关系所属单位负责。即由中标人负责采购及发放。  5.若服务期间发生的各种工伤、生产安全事故，事故处理及赔偿均由中标人负责，采购人免予承担一切责任。中标人负责贯彻实施好国家及当地安全系统运维服务规定，排除安全隐患，注意运维安全，保证服务人员具备相应的资质要求，佩证上岗。如服务期间出现财产损失或人身损害等安全事故由中标人负责，造成采购人损失，由中标人承担赔偿责任。  6.中标人执行采购人关于运维制服、外勤工作服款式、颜色的规定，采购由中标人直接负责。  7.所涉及的安全生产费用由中标人负责，采购人的委托运维价格已含从业人员安全教育培训、劳动防护用品费用等。 |  |  |  |  |  |

**注：1.此表仅作为汇总参与评审的10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10分（计算得分按四舍五入保留2位小数）；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。**