

采购包 1：2026-2028 年度智慧安防小区运维服务项目

服务内容及要求

1. 项目总体内容

1.1 服务内容概述

本次运维服务覆盖 773 个智慧安防小区，共计 3514 个前端点位，其中：

（1）前端视频采集设备：人脸门禁刷卡一体机 168 台、摄像头 3346 个（含人脸抓拍摄像机 2397 台、车辆抓拍摄像机 864 台、非机动车车道摄像机 85 台）。

（2）网络链路：3514 条前端至平台侧视频回传链路。

（3）供电系统：3514 套前端点位供电设施。

（4）箱体设施：773 个设备箱及配套环境。

（5）杆体及安装结构：773 套杆体、横臂及支架。

（6）光猫/ONU 及网络设备：3514 套前端接入网络设备。

（7）前端点位在日常使用中，因为特殊情况需要进行的迁改，供应商每年提供≥600 个点位的移点、换臂、降臂、杆体和外观维护服务。迁改费用包括在服务费中。

★1.2 主要服务清单汇总

（1）前端视频采集设备运维

序号	服务项目	服务内容	数量	单位
1	人脸门禁刷卡一体机运维	外观检查、功能检测、读卡模块清洁、固件升级	168	台
2	人脸抓拍摄像机运维	图像质量维护、镜头清洁、红外夜视、参数调试	2397	台
3	车辆抓拍摄像机运维	车辆捕获率检测、车牌识别率维护、图像质量	864	台
4	非机动车车道摄像机运维	画面角度调整、目标抓拍功能维护	85	台
5	视频诊断平台软件升级及授权扩	视频诊断平台软件升级、授权扩容、质量检测、录像诊断及运行统计服	1	套

	容	务		
--	---	---	--	--

(2) 网络链路传输服务

序号	服务项目	服务内容	数量	单位
1	前端网络链路运维	光纤链路巡检、光功率检测、专线接入保障	3514	条
2	光猫/ONU 运维	设备状态巡检、光功率检测、MAC 白名单管理	3514	台
3	网络安全接入保障	IPSec VPN/SSL VPN 通道维护、加密传输保障	1	项

(3) 供电系统运维

序号	服务项目	服务内容	数量	单位
1	供电系统运维	市电输入检查、电源适配器更换、空开及接地维护	3514	套

(4) 箱体设施运维

序号	服务项目	服务内容	数量	单位
1	箱体设施运维	防水密封、线缆整理、散热除尘、锁具维护	773	个

(5) 杆体及安装结构运维

序号	服务项目	服务内容	数量	单位
1	杆体及安装结构运维	垂直度检测、紧固检查、防锈处理、防雷接地	773	套

(6) 服务管理

序号	服务项目	服务内容	数量	单位
1	远程巡检服务	平台告警监控、在线率统计、远程故障恢复	3514	点
2	现场巡检服务	综合检查、预防性维护、隐患登记	3514	点
3	故障响应服务	30 分钟响应、2 小时到场、重点保障点位 8 小时内处理完成、普通点位 24 小时内处理完成	1	项

4	应急保障服务	重大活动、节假日、灾害天气 7× 24 值守	1	项
---	--------	---------------------------	---	---

★2. 服务模式

本项目采用综合运维模式，以“点位综合运维+网络侧协同支撑+工单闭环管理+专项保障机制”的总体架构，由运维服务单位提供前端设备、网络链路、供电、箱体、杆体、光猫/ONU 等以上网络设备的全链条运维服务，形成完整服务闭环。

★3. 服务目标

以“视频业务可用、链路传输稳定、供电安全可靠、点位设施完好、运维过程闭环”为总体目标，建立面向前端感知点位的综合运维服务体系。按照四川省公安厅、成都市公安局智慧安防小区考核及民生目标考核要求，本项目运维服务应重点实现以下目标：一是确保智慧安防小区建成接入率达到并持续保持 100%，即成华区现有 773 个智慧安防小区均有摄像头组成的前端感知设备接入智慧安防小区平台。各小区接入的摄像头应能够在平台正常注册、在线呈现并按权限调用，不得因运维原因出现小区整体未接入、整体脱网或长期失联。对设备更换、点位迁改、链路调整、平台参数变更等以上情形，应同步完成设备接入配置、基础信息更新和平台侧验证，确保小区接入覆盖不减少、接入关系准确、接入状态真实有效。二是保障分局智慧安防小区系统整体运行完好，持续提升前端设备在线率、视频图像可用率、网络链路稳定性和故障处置及时性，及时治理离线、黑屏、卡顿、图像质量下降、链路抖动问题等以上问题，确保各项指标满足四川省公安厅、成都市公安局月度考核要求，并力争在成都市公安局考核中保持前列。三是将系统连续运行和公安业务不中断作为刚性指标。运维期间应建立 7×24 小时故障受理、监测预警、快速响应、应急处置和闭环复盘机制，发生设备、供电、网络或平台接入异常时，应立即采取修复、替换、临时保障措施，最大限度缩短业务中断时间。总体核心目标为：设备不断供、网络不断网、业务不停摆。

目标类别	具体目标
业务可用目标	保障摄像头设备正常运行，视频能够稳定调阅、正常回传、画面可用，解决离线、黑屏、卡顿等以上影响业务的问题。
网络稳定目标	保障点位至平台的链路传输稳定，对光纤、ONU/光猫、交换

目标类别	具体目标
	设备、专线或 PON 接入链路开展日常维护和故障排查。
供电可靠目标	保障前端点位供电连续、接口稳固、防雷接地有效，解决断电、跳闸、适配器损坏、PoE 异常等以上问题。
设施完好目标	维护杆体、支架、横臂、防水密封和现场安装环境，排查因物理设施损坏导致的故障。
闭环管理目标	对巡检、报障、派单、维修、更换、验证、回访、归档进行全过程管理，形成可追溯服务记录。

★4. 服务原则

项目实施过程中须坚持以下服务原则，确保综合运维服务有组织、有标准、有记录、有结果。

(1) 以业务可用为最终判断标准。故障修复不能只看设备是否通电或网络是否连通，还要确认视频画面是否可用、平台是否能够调阅。

(2) 以端到端排障为基本方法。对摄像机、供电、链路、光猫/ONU、交换设备、箱体杆体和平台接入进行系统判断，避免片面归因。

(3) 以预防维护降低故障发生。通过巡检、清洁、紧固、防水、防雷、线缆整理、光功率检测、供电检查等以上手段提前治理隐患。

(4) 以数据化管理推动持续优化。通过月报、台账、工单、故障分析和隐患清单，将运维服务转化为可评估、可改进的管理成果。

5. 前端视频采集设备运维服务

5.1 前端视频采集设备运维对象及技术要求清单

本清单中的数量（单位）为纳入运维范围的设备或服务规模；参数要求用于对现有设备维护、兼容适配及软件授权/部署。

序号	服务项目	服务内容	★数量	★单位	参数要求
1	人脸门禁 刷卡一体机 运维	外观检查、 功能检测、 读卡模块 清洁、固件	168	台	1. 支持人脸识别、身份验证、通行管理； 2. 识别距离支持 0.3m-3m； 3. 本地人脸库支持≥2 万人；

		升级		4. 支持双摄设计，摄像头像素≥ 200 万像素，采用无补光灯设计； 5. 支持环境照度 0.001lux 时能正常进行人脸识别； 6. 人脸识别终端机身厚度≤ 26 mm； 7. 屏幕≥ 7 英寸触摸屏，屏幕分辨率$\geq 1024*600$，屏幕亮度$\geq 550\text{cd}/\text{m}^2$； 8. 人脸识别核验响应速度$\leq 300\text{ms}$，暗光：$\leq 100\text{ms}$，强光：$\leq 150\text{ms}$，逆光：$\leq 100\text{ms}$； 9. 支持双目深度活体检测，有效防御照片、电子屏、视频形式的非活体攻击； 10. 支持遮挡识别，在戴墨镜、戴帽子、蓄须遮挡情况下依然保持精准识别； 11. 支持离线识别，设备在网络离线情况下人脸识别正常运行，支持断网续传； 12. 具备不低于 IP66 和 IK07 防护等级，可以安装于室内或者室外； 13. 支持设备强拆、强制开门、非活体攻击异常报警； 14. 为满足与门禁系统对接，要求人脸识别终端支持韦根接口、485 接口、继电器接口、I/O 接口、USB 接口、网络接口；支持通过韦根接口控制门禁控制器开门，韦根支持
--	--	----	--	---

					26 位、32 位和 34 位格式； 15. 为满足个性化展示需要，需要用户自定义识别成功后屏幕显示的信息，其中用户的图片、姓名、工号、部门、身份证、职位可以选择是否展示，额外可以针对特定用户展示欢迎语。
2	抓拍摄像机运维	人脸抓拍摄像机图像质量维护、镜头清洁、红外夜视、参数调试+车辆抓拍摄像机车辆捕获率检测、车牌识别率维护、图像质量；非机动车车道摄像机画面角度调整、目标抓拍功能维护	3346	台	1. 不小于 1/1.8 英寸 400 万像素 CMOS 传感器； 2. 支持三码流同时输出，主码流最高分辨率$\geq 2688 \times 1520@25\text{fps}$； 3. 支持 H. 265、H. 264 编码方式； 4. 支持智能算法云端管理功能，支持在算法仓平台对摄像机算法进行加载、升级，加载或升级期间视频画面不中断； 5. 支持混行检测抓拍、关联抓拍； 6. 支持人脸优选抓拍、人脸属性提取； 7. 支持视频结构化，行人、机动车、非机动车的属性提取； 8. 支持区域人数统计、客流统计； 9. 支持 AI Smart 事件，在 Smart 智能基础上，可仅针对人体、机动车、非机动车进行智能触发，过滤掉其他物体干扰； 10. 支持 Micro SD 卡扩展，支持的最大存储卡容量不低于 256GB； 11. 支持超宽动态、背光补偿、强

				光抑制、3D 降噪、电子防抖、数字透雾； 12. ROI 支持不少于 8 个感兴趣区域； 13. 支持$\geq$IP67 防护等级； ★14. 支持 GB 35114-2017《公共安全视频监控联网信息安全技术要求》中的 A 级安全能力。
3	视频质量检测服务	智能视频质量诊断、录像完整性与可阅性监测、系统运行指标统计及部署调试服务	1	套 ★1. 配置国产处理器$\geq$2 颗(单处理器核数$\geq$24 核、主频 2.1GHz)，支持超线程； 2. 配置$\geq$128G DDR5 内存，速率最高支持 5600MT/s； 3. 配置不低于 3.84TB SSD 硬盘$\geq$4 个，不低于 960GB SSD 硬盘$\geq$2 个； ★4. 配置 1 张国产 GPU 卡，单卡算力不低于 192 TOPS（INT8）、18 TFLOPS（FP32），单卡功耗$\leq$75W（供应商需在投标文件中提供 GPU 参数配置的官网截图并进行电子签章）； 5. 支持对视频抖动检测、条纹干扰检测、视频信号丢失检测、视频遮挡检测、视频卡顿（冻结）检测、视频对比度异常检测、亮度异常（过亮/过暗）检测、噪声干扰检测、颜色异常检测、清晰度异常检测、场景变化检测、强横纹干扰检测、滚动条纹检测、横波干扰检测；

				6. 支持录像完整性的诊断，支持历史录像可调阅性监测； 7. 支持点位数、联网率、可用率、达标率、在线率、维保到期情况、系统建设情况等统计； ▲8. 支持单组件业务进程出现故障时可在 20 秒时间内完成业务恢复（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ▲9. 单节点支持不少于 200 个容器同时运行，支持对容器的资源性能进行阈值设置（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ★10. 对成华智慧安防小区接入平台云资源池进行授权扩容，扩容数量不少于 2 个 CPU 授权，并进行统一纳管（供应商需在投标文件中提供书面承诺函并进行电子签章，承诺函格式自拟）； ★11. 视频诊断软件支持容器化部署到成华安防小区接入平台并完成对接，部署后各节点 CPU、内存压力均衡（供应商需在投标文件中提供书面承诺函并进行电子签章，
--	--	--	--	---

					承诺函格式自拟)。
--	--	--	--	--	-----------

★5.2 前端视频采集设备运维要求及标准

前端视频采集设备运维应围绕视频业务连续运行和前端感知能力稳定发挥开展，重点保障设备接入状态、视频回传效果、抓拍数据质量和平台调用能力满足实际业务使用要求。运维单位应结合不同点位的业务属性、使用频次、覆盖范围和重要程度，建立差异化维护策略，对重点区域、重点通道、人员车辆出入口等关键点位实行优先保障，确保前端采集设备能够持续支撑治安防控、数据采集和日常管理需要。

前端视频采集设备运维应实行台账化、标准化和闭环化管理。运维单位应对设备基础信息、运行状态、参数配置、故障处置、设备更换和维护结果进行记录，确保设备状态可查询、维护过程可追溯、故障处理可复核。涉及设备配置调整、设备替换、点位变更或接入参数修改的，应按照采购人管理要求进行确认和登记，避免因配置不一致、信息不同步或操作不规范影响平台侧应用。

为保证前端视频采集设备在不同场景下达到稳定、清晰、可用的运行效果，运维过程中应根据点位用途、现场光照、网络承载、存储要求和智能识别需求，对设备关键参数进行规范化调试。具体参数调试标准如下：

参数类别	调试要求
分辨率/帧率	按监控需求设置，核心点位优先保证清晰度和流畅性，同时兼顾带宽与存储。
曝光/白平衡	根据日夜光照变化优化，避免画面过亮、过暗、偏色。
红外参数	调整补光强度和切换阈值，避免红外过曝或照射不足。
编码码率	在保证画质前提下降低带宽占用，优先使用高效编码。
智能规则	按现场目标区域设置检测范围和灵敏度，减少误报漏报。

★5.3 前端视频采集设备运维执行要求清单

序号	服务要求	执行频次	输出成果
1	设备在线状态核查	远程每日不少于1次，现场巡检 每月不少于1次	在线率统计、异常 点位清单
2	图像质量巡查	远程每周不少于1次，重点点位 每周不少于2次	截图记录、图像质 量问题台账

序号	服务要求	执行频次	输出成果
3	镜头、防护罩清洁及角度校正	现场每季度不少于 1 次,发现污损、偏移或遮挡时即时处理	清洁记录、调整前后照片
4	智能抓拍、识别及规则功能验证	每月不少于 1 次,重大保障前专项复核 1 次	抓拍测试记录、规则参数记录
5	固件版本核查与配置备份	每半年不少于 1 次,配置变更前各备份 1 次	版本清单、配置备份记录
6	重复故障点位复查	每月汇总分析 1 次,整改后 7 日内复查 1 次	复查记录、整改闭环单

★5.4 前端视频采集设备运维服务内容

(1) 外观与安装检查

结合现场巡检每月不少于 1 次检查相机外壳、防护罩、镜头、支架、杆体、设备箱和固定螺丝是否完好。发现松动、偏移、锈蚀、破损、密封失效或人为破坏风险时即时处置；现场无法完成的，当日形成问题记录并报采购人。室外点位同步检查进水痕迹、密封胶老化、防雷接地和线缆固定情况。

(2) 图像质量维护

图像质量巡查远程每周不少于 1 次，重点点位每周不少于 2 次；维护内容包括清洁镜头、防护罩，调整焦距、曝光、白平衡、宽动态、降噪和码率，处理模糊、偏色、过曝、欠曝、卡顿、花屏、遮挡问题。对采购人规定的核心点位应每周不少于 2 次截图留存，便于对比画面质量变化。

(3) 红外与夜视功能维护

夜间或低照度环境下检查红外灯、补光灯、ICR 切换、红外照射范围和夜视画面噪点。若出现红外不亮、过曝光白、近距离反光、夜间频繁重启等以上问题，将同时检查供电功率、安装角度、反射面、电源线径和红外参数。

(4) 智能功能维护

针对移动侦测、越界检测、区域入侵智能规则等以上智能规则，每月不少于 1 次核查检测区域、灵敏度、告警联动和平台接收情况，重大保障前专项复核 1 次。发现误报、漏报或无响应时，先核对规则配置和现场环境，再检查固件版本、网络传输和设备算力状态。

（5）固件升级管理

固件升级遵循“版本核查、配置备份、低峰实施、升级验证、记录归档”的流程。仅使用与设备型号和硬件版本匹配的固件包，升级期间不得断电、断网。批量升级应分批进行，先试点、后推广；如升级失败，应按回退预案恢复原版本并联系厂商分析原因。

（6）巡检与预防性维护

前端视频采集设备巡检应结合远程巡检和现场巡检同步开展。远程巡检主要通过平台查看摄像机在线状态、视频预览状态、录像回传状态、码流状态、设备告警、图像清晰度、画面遮挡、黑屏、花屏、卡顿和抓拍功能是否正常，发现影响视频业务可用性的问题。

现场巡检应重点检查摄像机外观、镜头及防护罩清洁度、安装角度、支架固定、线缆连接、防水密封、补光灯或红外灯工作状态、设备运行温度和周边遮挡情况。对镜头污损、画面偏移、支架松动、线缆松脱、外壳破损、补光异常、遮挡物影响画面等以上问题，应现场进行清洁、调整、紧固、恢复或登记上报。

预防性维护应重点做好镜头和护罩清洁、图像参数复核、安装角度校正、支架螺丝紧固、补光效果检查、设备运行状态观察和历史故障点位复查。对重点区域摄像机、频繁离线摄像机、画面质量下降点位和历史重复故障点位，应纳入重点关注清单，结合巡检记录和工单数据持续跟踪，降低前端视频采集设备故障率，保障视频画面长期清晰、稳定、可用。

头—安全联网设备—VPN 加密链路—中心汇聚平台—业务应用平台”的整体网络架构。

6.3 网络链路运维主要服务清单

序号	服务项目	服务内容	★数量	★单位	参数要求
1	前端网络链路运维	光纤链路巡检、光功率检测、专线接入保障	3514	条	1. 上下行带宽 $\geq 20\text{M}$ 。
2	光猫/ONU 运维	设备状态巡检、光功率检测、MAC 白名单管理	3514	台	1. 下行 2.488Gbps、上行 1.244Gbps。 2. 光口：SC/UPC；Tx1310nm、Rx1490nm；接收灵敏度 -28dBm 。 3. 网口：1 $\times$ FE(百兆)。 4. 供电：12V/1A；尺寸 100 $\times$ 80 $\times$ 26mm（ $\pm 3\text{mm}$ ）；重量 $<220\text{g}$ 。
3	网络安全接入保障	安全网关通道维护、加密传输保障	1	项	★1. 安全网关应采用国产 CPU 架构及国产操作系统； ▲2. 国密 IPsec 加密速率 $\geq 1.9\text{Gbps}$ ，SSL 并发连接数 ≥ 40 万，SSL 每秒新建连接数 ≥ 1 万（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ▲3. 预充注量子密钥 $\geq 10\text{M}$ ，

				且支持根据配置的时间周期自动更新加密工作密钥，最高密钥更新频次不低于 5 分钟/次（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ▲4. 支持 PQC+SM2 混合算法套件，并应用于 IPSec VPN 及 SSL VPN 协议，实现 SM2+PQC 混合加密（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ▲5. 支持 PQC+SM2 混合证书体系，平滑兼容现有 SM2 证书体系（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进行电子签章，对该技术要求进行佐证。）； ▲6. 支持基于网络层、传输层的净荷数据加密方式，可实现对业务数据的无感知加密、解密（供应商需在投标文件中提供第三方检验检测机构出具的检验检测报告扫描件并进
--	--	--	--	---

					行电子签章，对该技术要求进行佐证。）； ▲7. 满足 GM/T 0023-2023《IPSec VPN 网关产品规范》、GM/T 0025-2023《SSL VPN 网关产品规范》及 GM/T 0028-2024《密码模块安全要求》（二级）要求，具备商用密码检测认证中心（含原国家密码管理局商用密码检测中心）颁发的《商用密码产品认证证书》（供应商需在投标文件中提供商用密码检测认证中心（含原国家密码管理局商用密码检测中心）颁发的《商用密码产品认证证书》扫描件并进行电子签章）； ▲8. 产品具备 IPv6 相关认证证书（供应商需在投标文件中提供 IPv6 相关认证证书扫描件并进行电子签章）。
--	--	--	--	--	---

★6.4 网络链路运维要求

网络链路是前端视频回传的通道，链路质量直接影响视频是否能够实时查看、录像是否完整、画面是否卡顿。除提供网络链路运维服务外，项目团队还应根据现场视频回传需求，提供专网链路接入及传输通道保障服务，确保前端摄像机至平台侧之间具备稳定、可靠、安全的传输能力。同时，针对前端视频数据跨网络回传、专网接入和平台侧访问的安全要求，应在链路边界侧配置具备加密传输、身份认证、访问控制和隧道化传输能力的安全接入设备，保障视频数据在传输过程中的机密性、完整性和接入可信性。

链路环节	维护重点	服务措施
现场网线链路	网线、水晶头、端口接触、线缆老化、防水接头	重新压接、更换网线、端口测试、防水处理
光纤尾纤及跳线	尾纤弯折、端面污染、光功率、跳接标签	清洁端面、规范盘纤、更换尾纤、测试光功率
PON 接入链路	ONU 注册、PON 灯状态、OLT 侧信息、LOID/SN 绑定	核查注册信息、排查光路、重启或更换 ONU、联动接入网支撑
OTN/专线链路	链路告警、传输质量、端口状态	网络侧排障、传输支撑、链路恢复和质量观察
安全加密传输通道	加密通道状态、证书状态、密钥更新、身份认证、访问控制、传输完整性	建立和维护安全加密通道，核查证书与密钥状态，支持密钥周期更新，联动网络侧处理加密通道异常，保障视频数据安全回传

★6.5 网络链路运维执行要求清单

序号	服务要求	执行频次	输出成果
1	链路连通性和业务可用性巡检	远程每日不少于 1 次，发现离线或卡顿即时派单	链路巡检记录、异常点位清单
2	光功率、尾纤及跳线检测	现场每季度不少于 1 次，故障处理时同步检测	光功率测试记录、尾纤跳线处理记录
3	光猫/ONU 注册状态核查	每周不少于 1 次，批量离线或告警时即时核查	ONU 状态清单、注册异常处理记录
4	PON/OTN/专线网络侧协同巡查	每月不少于 1 次，重大保障前专项核查 1 次	网络侧协同记录、链路质量分析
5	安全加密通道、证书及密钥状态检查	每月不少于 1 次，证书或密钥变更前后专项复核	通道状态记录、证书/密钥检查记录
6	网络隐患治理与复盘	每月形成 1 次网络隐患清单	隐患清单、整改闭环

序号	服务要求	执行频次	输出成果
		单，整改后 7 日内复查	环记录

★6.6 网络链路运维服务内容

（1）带宽保障

前端点位至平台侧的视频回传链路主要为保障视频实时预览、录像回传、平台调阅、远程运维和告警数据传输业务稳定运行。项目团队将围绕摄像机至现场交换设备、现场交换设备至光猫/ONU、ONU 至接入网、接入网至汇聚/传输网络、传输网络至平台侧的全路径开展链路接入调测、运行维护和故障排查。对于专网链路，项目团队负责链路资源协调、接入保障、传输配置、连通性测试及后续运行保障，确保视频业务具备独立、稳定的网络承载能力。

（2）故障排查协作

对于可由项目现场人员处理的接头、尾纤、网线和端口等以上问题，现场直接修复；对于涉及接入网、传输网、专线资源或上联链路的问题，立即联动网络侧支撑进行排障，形成从现场到网络侧的闭环处理。

（3）光猫/ONU 及前端网络设备运维

将光猫/ONU、交换机、PoE 设备纳入网络链路运维范围，建立设备台账，记录设备型号、序列号、安装位置、接入链路、端口用途、电源方式和更换记录。故障处理时结合指示灯判断、端口测试、光功率测试、替换验证和网络侧信息核查进行定位，避免盲目更换。

（4）巡检与预防性维护

通过远程网管、平台告警和现场测试定期核查链路连通性、ONU 注册状态、光功率、端口状态、跳纤标签、尾纤弯折、线缆防水和加密通道状态。对光衰偏高、端口频繁闪断、PON 注册异常、专线质量波动和加密通道异常的点位建立网络隐患清单，联动网络侧支撑闭环治理。

★7. 供电系统运维服务

7.1 供电系统运维服务要求

供电系统是前端点位稳定运行的基础。供电异常通常会表现为设备离线、摄像机频繁重启、光猫/ONU 掉线、交换机端口不稳定、夜间补光无法启动。将把供电检查纳入日常巡检和故障排查必查项。对于供电类故障，坚持安全优先原则。

涉及带电操作、高压风险、外部电源产权或需要专业电工处理的事项，现场人员将做好安全隔离和问题确认，并按采购人要求协调相关单位处理。在不违反安全规范和面对不可抗力因素的前提下，优先通过更换适配器、恢复空开、临时供电保障等方式恢复业务。

7.2 供电系统运维执行要求清单

序号	服务要求	执行频次	输出成果
1	前端点位供电状态检查	现场每月不少于 1 次，故障工单处理时同步检查	供电巡检记录、电压测试记录
2	空开、插座、接线端子紧固检查	每季度不少于 1 次，发现松动、发热或跳闸即时处理	紧固维护记录、隐患照片
3	电源适配器、PoE 供电模块检测	每季度不少于 1 次，频繁重启点位即时检测	检测记录、更换记录
4	防雷接地检查	每半年不少于 1 次，雷雨季前专项检查 1 次	接地检查记录、防雷隐患清单
5	供电隐患整改复查	整改完成后 7 日内复查 1 次	复查记录、闭环确认单

7.3 供电系统运维服务内容

包括市电输入、空开、插座、接线端子、电源适配器、PoE 供电、光猫电源、交换机电源、接地线和电源线缆。现场人员将通过目测、测量、通断测试和负载判断等以上方式确认供电状态，对接头松动、空开跳闸、电源损坏、线缆破损、设备过热等问题及时处置。

维护对象	维护内容	异常表现	处置内容
市电输入	检查电压、接线、空开状态和供电连续性	点位整体断电、空开跳闸、电压异常	恢复供电、查找跳闸原因、形成供电隐患记录
电源适配器	检查输出电压、发热、接口松动、老化损坏	摄像机或光猫反复重启、无法上电	更换适配器，整理线缆并固定接口
PoE 供电	检查 PoE 端口功率、供电距离、端口状态	摄像机间歇掉线、供电不足、端口失	调整端口、更换 PoE 交换机或供电

维护对象	维护内容	异常表现	处置内容
		效	模块
箱内强弱电	检查强弱电分离、绝缘保护、线缆固定	线缆混乱、接触不良、短路风险	规范整理线缆，消除安全隐患

★8. 箱体设施运维服务

8.1 箱体设施运维服务要求

箱体设施运维应以保障前端设备稳定运行环境为目标，按照“环境安全、线缆规范、设备有序、防护有效、隐患可控”的原则开展。在日常巡检、故障处理和专项保障过程中关注箱体运行状态，防止因箱体环境恶化引发设备离线、供电异常、链路中断或安全隐患。

箱体设施维护应坚持预防为主、处置和闭环管理。对现场能够处理的一般问题，应在巡检或维修过程中同步完成整改；对涉及箱体更换、安装位置调整、严重破损或存在安全风险的问题，应在发现后 30 分钟内形成隐患记录并向采购人报备，同时提出整改建议。所有箱体类问题应纳入运维台账管理，做到问题可追溯、处置有记录、整改有反馈。

8.2 箱体设施运维执行要求清单

序号	服务要求	执行频次	输出成果
1	箱体外观、箱门、箱锁及密封检查	现场每月不少于 1 次，发现破损或进水风险即时处理	箱体巡检记录、问题照片
2	箱内清洁、除尘、防虫及散热检查	每季度不少于 1 次，高温季节或故障点位增加检查	清洁维护记录、散热检查记录
3	线缆整理、标签更新及盘纤规范检查	每季度不少于 1 次，设备更换或线路调整后即时整理	线缆整改记录、标签台账
4	防水、防潮和进线孔封堵检查	每季度不少于 1 次，汛期或暴雨后专项检查 1 次	防水处理记录、隐患清单
5	箱体接地、防盗和警示标识检查	每半年不少于 1 次，发现缺失或损坏即时恢复	安全检查记录、恢复记录

8.3 箱体设施运维服务内容

设备箱是前端点位网络设备、电源设备和连接线缆的重要承载空间。箱体防水、防尘、散热、防盗和线缆规范程度直接影响摄像机、光猫/ONU、交换机和电源设备的长期运行。在现场巡检中重点检查设备箱状态。箱体维护不只是外观维护,更重要的是为内部网络和供电设备提供稳定环境。对于箱体进水、线缆混乱、尾纤弯折、设备堆叠、散热不良等以上问题,将在现场能处理的范围内立即整改;对于箱体严重破损、安装位置不合理或需要更换的情况,形成隐患报告和整改建议。

箱体维护内容包括箱体外观及密封性检查、箱体内外清洁、线缆整理与标识更新、散热与防尘检查、防水防潮检查、箱体锁具及防盗检查、接地及防雷设施检查。

巡检与预防性维护应同步关注箱体防水、防尘、防虫、散热、防盗、接地和线缆规范。对箱体进水、密封条老化、进线孔封堵不严、尾纤弯折、设备堆叠、标签缺失等以上问题,能现场处理的立即整改;需要更换箱体或涉及施工改造的,形成隐患清单并报采购人确认。

箱体项目	检查内容	维护措施
箱体外观	箱门、箱锁、铰链、锈蚀、变形、破损	修复或更换锁具, 处理锈蚀, 记录破损情况
密封防水	密封条、防水胶、进线孔、箱体底部积水	补强密封, 整理进线孔, 清理积水和潮湿隐患
箱内环境	灰尘、虫害、杂物、过热、设备摆放	清洁箱体, 整理设备, 改善散热和通风
线缆规范	强弱电分离、标签、扎线、盘纤、接头固定	重新整理线缆, 补充标签, 规范盘纤和绑扎
安全防护	箱体接地、防盗、防触电、警示标识	恢复接地连接, 补充警示标识, 消除安全风险

★9. 杆体及安装结构运维服务

9.1 杆体及安装结构运维服务要求

杆体及安装结构运维应以保障前端摄像机安装稳固、视角稳定和现场作业安

全为目标。对不影响结构安全的一般性问题，应立即进行现场处理并做好记录；对可能影响杆体稳定、设备安全或公共安全的问题，应立即采取必要的现场风险提示措施，并立即向采购人报备，纳入专项隐患清单跟踪处理。涉及杆体更换、基础修复、移点、换臂、降臂或其他施工类事项的，应按照采购人及相关管理部门要求组织实施。

杆体及安装结构运维质量应满足前端视频采集角度稳定、设备安装牢固和现场安全可控的要求。运维单位应结合日常巡检、故障工单和重点保障任务，对易受外力影响、历史故障频发、周边环境变化较大的点位进行重点管理，减少因安装结构问题造成的画面偏移、设备损坏和安全风险。

9.2 杆体及安装结构运维执行要求清单

序号	服务要求	执行频次	输出成果
1	杆体垂直度、基础及地脚螺栓检查	每半年不少于1次，外力碰撞或极端天气后即时检查	杆体巡检记录、结构隐患清单
2	横臂、支架、抱箍和固定件紧固检查	每季度不少于1次，画面偏移或设备晃动时即时处理	紧固维护记录、调整前后照片
3	杆体、横臂及支架防锈和外观维护	每半年不少于1次，发现锈蚀、脱漆或变形即时登记处理	防锈维护记录、外观维护记录
4	防雷接地连接检查	每半年不少于1次，雷雨季前专项检查1次	接地检查记录、防雷隐患记录
5	移点、换臂、降臂及杆体外观维护	每年提供不少于600个点位的移点、换臂、降臂、杆体和外观维护服务	迁改记录、施工照片、点位台账更新
6	视角复核和遮挡治理	重点点位每月不少于1次，遮挡变化或业务要求调整时即时复核	视角复核记录、遮挡治理记录

9.3 杆体及安装结构运维服务内容

维护对象	检查重点	处置要求
立杆	垂直度、锈蚀、变形、外力碰撞、	记录隐患，能加固的立即加

维护对象	检查重点	处置要求
	基础开裂	固，重大隐患上报客户
横臂和支架	松动、变形、锈蚀、焊点异常、 安装角度	紧固螺栓、调整角度、并提出 更换建议
抱箍和固定件	抱箍松动、螺母缺失、卡件老化	补齐固定件，重新紧固，防止 设备移位
基础和地脚	基础破损、地脚螺栓锈蚀、地面 沉降	现场记录并提出专项整改建 议
接地连接	杆体接地线连接、防雷引下线状 态	恢复连接、紧固端子、纳入防 雷检查

杆体维护内容包括杆体垂直度及基础检查、横臂及抱箍紧固检查、支架及安装件锈蚀检查、防雷接地检查、杆体标识及标牌检查。

对杆体类问题，将区分一般维护和结构性整改。一般松动、轻微锈蚀、支架角度偏移等以上问题可由现场维护人员处理；涉及杆体更换、基础修复、大型施工或安全风险较高的问题，将立即上报采购人并配合制定整改方案。

9.4 杆体迁改及巡检预防服务

针对前端点位在日常使用中因道路施工、遮挡变化、管理要求调整或视角优化等以上特殊情况需要进行的迁改，至少包括移点、换臂、降臂、支臂调整、拆点恢复和基础设施配合整改。

★10. 故障响应与闭环管理服务

故障处理覆盖前端视频采集设备、网络链路、供电系统、箱体设施、杆体安装结构及网络接入设备。故障来源包括客户报障、平台告警、远程巡检发现、现场巡检发现、网络侧告警、重大活动保障检查发现以及采购人反馈。

故障受理后，供应商调度人员记录故障时间、点位名称、故障现象、影响范围、联系人、初判类型和紧急程度，并生成工单。对“全部区域无法查看”“多点同时离线”“重点区域视频中断”等以上问题，优先判断网络链路、供电系统或平台接入侧原因并启动升级响应；对单点离线、画面黑屏、光猫离线、箱体进水、杆体倾斜等以上问题，安排专业人员现场处置。

响应时限执行 30 分钟内明确响应和安排、2 小时内到达现场、重点保障点

位 8 小时内处理完成、普通点位 24 小时内处理完成的要求。因市政施工或不可抗因素无法按时修复的，立即向采购人报备并按采购人要求采取迁移、临时保障或后续恢复措施。

故障恢复后开展业务验证和记录归档，确认视频正常显示、图像清晰、平台可调阅、网络稳定、光猫/ONU 注册正常、供电恢复、箱体杆体无遗留风险。对重大故障和重复故障开展复盘，形成原因分析、处置过程、恢复时长、暴露问题和改进措施，并纳入月度服务报告。

★11. 服务管理

11.1 组织管理

(1) 运维服务所有人员应当坚决遵守成都市公安局成华区分局的各项相关规定，无任何前科和违法犯罪记录；应当具备保密意识和能够承担各项维护服务工作任务的专业技术能力。

(2) 供应商在响应文件中为本项目指派的全部运维团队人员（项目经理 1 名、技术负责人 1 名、运维工程师 4 名、运维网络安全工程师 2 名、应急支援后备团队不低于 3 名）在合同签订前，供应商必须安排所有人员本人携带有效身份证件原件，到采购人指定地点进行现场集中核验；对应岗位有专业资格或认证要求的人员，应同时携带相关证书原件。上述材料经采购人审查通过，且所有人员均完成背景审查并签署采购人要求的保密承诺书后，方可取得进入成都市公安局成华区分局提供现场服务的资格。（**供应商须在响应文件中提供书面承诺函并进行电子签章，承诺函格式自拟**）

(3) 通过审查的运维团队人员应当接受采购人为期不少于 3 天的维护服务工作规范、安全保密制度以及公安机关相关管理规定的教育培训。

(4) 供应商的运维团队人员均应经过不少于 15 天的试用期，在试用期间接受成都市公安局成华区分局相关管理部门的管理和考核。

(5) 通过试用期的运维团队人员应当接受成都市公安局成华区分局每季度定期考核管理工作。

(6) 运维团队人员应当严格遵守成都市公安局成华区分局各项规范化管理的规章制度，注重日常行为养成，如因违反成都市公安局成华区分局各项管理规定，将根据情节轻重扣减供应商维护服务评价成绩。

（7）运维团队人员应接受成都市公安局成华区分局相关管理部门的管理，除正常的人员离职外，供应商如需调派或调整应当得到成都市公安局成华区分局相关管理部门的书面同意方可。

（8）供应商应当建立运维团队人员储备库，至少确保服务团队各类人员 1:1 的储备数量，确保在任何时间和任何情况下（包括人员病事假、工休、调休）人员数量和质量，能够满足成都市公安局成华区分局随时提出的服务人员调整要求。

（9）供应商应当规范运维团队人员离职管理和离职教育，离职人员脱密期不少于 3 个月，离职人员必须分别与成都市公安局成华区分局和供应商签订离职保密责任书和承诺书，交回因履行维护服务工作办理的所有证照和可能持有的所有资料。

（10）供应商应当严格工作操作规程管理，承担相应管理责任，如发生因违反操作规程、安装调试、日常运行维护操作或操作不当造成设备损坏或停止服务的，应当按照成都市公安局成华区分局要求在规定时限内无条件恢复，并由供应商承担由此带来的全部责任和损失。

（11）供应商应当建立健全运维服务工作管理制度，落实完善维护服务管理工作措施，确保所有运维服务人员严格执行工作制度和流程，在工作时不得从事任何与成都市公安局成华区分局维护服务工作无关的事情，如发生违反项目方案要求和相关制度规范的情形将视情况扣减供应商维护服务评价成绩，以全力确保维护服务工作质量和工作效率。

（12）供应商应当按照人员管理要求提供运维服务所有人员相关资料供成都市公安局成华区分局审查，并组织开展相关教育培训和考试，正式履行合同时供应商配置的运维团队人员必须全部到位。

（13）供应商应当遵照公安信息安全相关规定及要求，每季度不少于 1 次组织数据安全及公安网络安全教育培训。正式履行合同期间，若出现公安网络及信息安全事故（包括但不限于公安工作数据泄露、公民个人信息泄露、公安内网“一机两用”及其他违法违规情况），成都市公安局成华区分局有权追究供应商及违法违规个人相关责任。若出现重大公安网络及信息安全事故（包括但不限于受到被立案为刑事案件、公安部点名通报等以上情况），成都市公安局成华区分局有

权终止合同，并按照合同总额的 10%收取赔偿金。

(14) 供应商运维团队人员需服从成都市公安局成华区分局的领导和管理，严格遵守人员管理、请销假和保密制度。采购人有权对项目人员现场服务情况进行监督，认为服务人员不能胜任工作要求时，有权要求供应商限期更换相关人员。对采购人明确要求现场保障的岗位或时段，供应商应确保相应人员到位；人员休假导致现场保障缺口时，应安排后备技术人员补位。服务期内未经采购人允许不得变更运维服务人员；服务周期内现场服务人员更换不得超过 2 人次。人员更换时必须完成全面工作交接，因工作交接不到位影响服务的，视为供应商违约，由供应商承担相应违约责任。

11.2 沟通机制

供应商与采购人需密切沟通，日常保持畅通的电话沟通渠道，重要事件采用函件方式沟通。成都市公安局成华区分局业务部门来函，供应商需在次日内对函件以正式函件的形式回函，回函中应对成都市公安局成华区分局业务部门函件要求内容作出回复，回复内容包含：工作办理计划、完成时间。并在回函后按回函承诺按时保质保量完成成都市公安局成华区分局业务部门的要求工作内容。

供应商需在智慧安防小区日常维护服务中向采购人提供一点服务响应，响应内容包括：一点业务咨询、一点业务受理、一点故障申告、一点计费结算、一点技术支持。在采购人重大安保任务或时间节点期间根据采购人通知安排维保人员 24 小时待命。

对于智慧安防小区点位故障，供应商保证 7×24 小时受理电话报障，成都市公安局成华区分局业务部门可通过智慧安防小区专用报障系统、微信工作群、供应商智慧小区项目经理电话进行故障申告，供应商需指定专门业务部门或专人为联系人，响应采购人要求。

11.3 培训服务

为确保智慧小区在验收后正常运行，根据成都市公安局成华区分局业务部门要求，供应商需按照采购人要求对采购人相关人员进行系统组成及原理、常用的维护操作方法、系统实际操作技能的培训。

11.4 应急保障

针对重大活动、重要会议、节假日安保、自然灾害、极端天气、大面积离线

和突发安全事件，将启动应急保障机制。应急保障强调提前准备、重点巡检、人员待命、备件前置、网络侧关注和快速恢复。

应急保障流程包括任务接收、保障范围确认、重点点位核查、人员和备件准备、现场或远程值守、突发故障处置、结果确认和总结报告。对于重大应急场景，项目经理负责统一协调，技术负责人负责技术判断和工单调度，运维工程师及运维网络安全工程师负责具体处置。

保障前：核查重点点位在线率、图像质量、链路状态、供电状态、光猫/ONU状态和箱体杆体隐患。

保障中：保持 7×24 响应，重点点位异常优先处理，网络侧关注链路告警，现场人员携带备件待命。

保障后：形成保障总结，说明发现问题、处理情况、遗留风险和后续优化建议。

11.5 备品备件与工具管理

供应商需结合项目设备类型、历史故障类型、点位重要程度和供应周期配置备件，若摄像机硬件发生损坏，则直接进行更换，并对备件进行入库、出库、使用、回收和盘点管理。

备件使用实行登记管理。每次备件出库需记录领用人、使用点位、备件型号、序列号、故障原因和旧件回收情况。更换完成后，维护人员应更新设备台账和备件台账，确保资产信息准确。

网络侧备品备件应覆盖前端接入、光路连接、链路传输、安全加密通道和现场检测工具等以上内容，用于支撑网络侧故障快速定位、替换验证和业务恢复。涉及网络侧设备产权、配置权限或上联资源调整的，应在采购人确认后联动网络侧支撑单位实施，避免因擅自变更影响现网业务。

★12. 安全性要求

12.1 信息安全与数据安全

前端视频感知点位涉及视频图像、点位信息、网络参数、设备账号和平台接入信息，将严格落实信息安全和保密要求。

运维人员不得擅自复制、下载、传播或泄露视频资料、点位资料、账号密码和网络配置。

设备账号和平台账号实行授权使用，避免默认密码、弱口令和多人共用账号。涉及网络配置变更、设备替换和平台参数调整的操作，应履行确认和记录流程。

服务报告中涉及敏感点位、截图或网络信息时，按客户要求进行了脱敏处理。人员变更、项目结束或权限调整时，及时配合客户进行账号和资料交接。

12.2 网络接入安全

采用前端网络接入设备（光猫）设置白名单的安全策略，将前端摄像机的MAC地址写入光猫白名单，其他设备在未得到白名单授权的情况下，无法通过网络设备直接接入网络；同时，针对非法访问能够进行预警提示。前端网络接入设备（光猫）如有WIFI功能，必须关闭。

12.3 现场作业安全

现场维护涉及登高、用电、道路周边作业和室外环境风险，必须执行安全作业规范。

涉及带电操作、高压风险、外部电源产权或需要专业电工处理的事项，现场人员将做好安全隔离和问题确认，并按客户要求协调相关单位处理。

严格执行登高作业安全规范，作业人员需佩戴安全帽、安全带等防护装备。

★13. 考核办法

本项目由采购人组织实施考核，自运维服务正式启动之日起按月设置考核周期，每个考核周期满分100分。其中，在线率及接入率项以100分为基准，按13.3（1）据实扣分；再在此基础减去“其他扣分项”（按13.3（2）…单项不作上限）。当月考核得分=在线率及接入率得分-其他扣分项累计扣分，最低为0分。当月考核得分低于80分（合格线）的，视为该周期考核不达标，按13.4相应比例执行。

13.1 考核依据

成都市公安局成华区分局成华区智慧安防小区建设项目方案。考核内容：服务响应时间、前端点位故障处理情况、后台存储情况、点位的标注、监控中心维护。

13.2 考核形式

考核每月进行一次，供应商的考核得分将作为每季度运维费用结算的重要依

据。

采购人应于次月第 5 个工作日内，按照考核标准完成上一考核周期服务质量考核及扣分确认，并由采购人相关部门根据考核结果确定该期运维费用下浮比例。

智慧安防小区运维服务项目月度考核表				
日期	点位总数	点位在线数	在线率	其他扣分项

合计	本月平均在线率为：xx % 其他扣分为：x 合计得分为：xx			
备注	1、周期考核得分 95 分（不含）以上，全额支付该期运维费。 2、周期考核 91-95 分，按照 95%比例支付该期运维费。 3、周期考核 86-90 分，按照 90%比例支付该期运维费。 4、周期考核 81-85 分，按照 85%比例支付该期运维费。 5、周期考核 80 分（含）以下，按照分数等比例支付该期运维费。 周期考核支付比例按 13.4 考核结果执行；打分标准详见 13.3。			

13.3 打分标准

（1）在线率及接入率考核如下：

本项目采用前端点位月平均在线率方式进行考核，采购人记录日在线数量并进行月平均数统计。如当月前端点位在线率达到 98%或以上，不扣分；如低于 98%，每降低 1 个百分点扣 1 分（下降不足 1 个百分点的，按 1 个百分点计扣）。

采购人每月对智慧安防小区建成接入率进行考核，接入率达到 100%不扣分；低于 100%的，每降低 1 个百分点扣 1 分（下降不足 1 个百分点的，按 1 个百分点计扣）。

（2）服务质量扣分项如下：

供应商每个考核周期应至少完成 1 次巡检，确保系统正常使用。采购人每个考核周期末对供应商巡检完成情况进行汇总，发现应巡未巡的，每发现 1 件扣 2 分。

采购人发生重大保障任务，供应商根据采购人要求派专人到现场全力配合，如有违反情况发生，发现一件扣 6 分。

监控保障系统中点位信息不全，造成出现故障无法正常报障，发现一件扣 2 分。

前端监控系统中，未经采购人同意，私自增加或减少点位，发现一件扣 3 分。

前端监控系统中，视频传输、应用、点位视频回放、点播或下载功能不能正常使用，发现一件扣 2 分。

前端监控系统中，图像储存低于 31 天，发现一件扣 2 分。

前端监控系统中，图像名称与图像实际情况不符，发现一件扣 1 分。

供应商工作人员将图像资料外泄，导致相关事件被公安部点名通报的，发现 1 次扣 20 分。

前端点位故障，未在规定时间内排障，发现一件扣 1 分。

前端点位摄像头严重污脏，影响正常使用，未在规定时间内清洁，发现一件扣 1 分。

监控中心故障，未在规定时间内排障，发现一件扣 4 分。

接采购人通知，供应商未按规定按时拆除前端点位，发现一件扣 2 分。

接采购人通知，供应商未按规定按时恢复已拆除的前端点位，发现一件扣 2 分。

供应商应及时更新优化升级前端监控系统版本，若发现使用版本未达到采购人书面确认的版本要求，发现一次扣 5 分。

以上考核以错误发现时间和后果出现时间为准，纳入该考核周期的考核得分。

13.4 考核结果

周期考核得分 95 分（不含）以上，为优秀级，全额支付该期运维费。

供应商周期考核分数 95 分（含）以下，采购人有权下浮一定比例支付运维费。运维费下浮比例后支付情况具体为：

（1）周期考核 91-95 分，按照 95%比例支付该期运维费。

（2）周期考核 86-90 分，按照 90%比例支付该期运维费。

（3）周期考核 81-85 分，按照 85%比例支付该期运维费。

（4）周期考核 80 分（含）以下，按照考核得分等比例支付该期运维费，采购人有权要求供应商限期整改；因数据安全风险事故或重大信息安全事件导致不

合格的，采购人有权按合同约定另行处罚、追究违约责任。

供应商连续两个考核周期的考核得分均 ≤ 80 分的，采购人有权单方面解除合同且不承担责任；由此造成的经济损失和法律责任由供应商自行承担，采购人有权视情节追究违约责任。

13.5 考核验收办法

针对本合同第 年度（ 年 月 日—— 年 月 日）履约情况进行考核打分。年度验收考核得分 > 80 分为通过， ≤ 80 分为不通过；不通过的，供应商应按采购人要求限期整改并重新考核；若仍不合格的，采购人有权立即终止合同。

年度验收考核表

编号	事项	考核指标	扣分细则	扣分
1	网络故障	供应商违反操作规程、未告知采购人而擅自割接电源或网络链路造成的网络故障及通信中断事故或其他人为原因造成的网络故障及通信中断事故。	出现一次扣1分；因擅自割接等造成重要业务中断的每次扣10分	
2	点位故障	纳入本项目运维范围的前端点位故障未按照日常维护要求时限恢复（市政施工或其他不可抗拒因素导致的故障须根据实际情况安排特殊处理且必须征得采购人同意）	出现一起扣0.1分；超过24小时未恢复的每起另扣1分	
3	数据故障	影响系统正常运行的关键数据处理设备或视频存储服务设备或视频存储服务器故障超过48小时未恢复	出现一起扣1分；关键数据处理设备或视频存储服务器故障超过48小时未恢复的每次扣10分	
4	系统故障	纳入本项目运维范围的系统及平台出现故障，不能按照项目要求正常使用，超过24	出现一起扣1分；核心系统超过48小时未恢复的每次扣10分	

		小时未恢复		
5	日常巡检	供应商在本服务年度内未每月对此次项目包含所有平台、设备及链路进行巡检，并向采购人提供巡检记录和整改报告（如记录和报告弄虚作假，一次性扣10分）	出现一起扣1分；巡检记录或整改报告弄虚作假的每次扣10分	
6	接入率下降	因供应商未按时响应、修复，导致建成接入率低于100%，超过24小时未恢复	出现一起扣1分；因供应商原因接入率持续下降且超过24小时未恢复的再扣5分	
年度验收考核得分：				

附注：年度验收考核表各项按次累计扣分，单项扣分不作上限限制。

本服务年度内发生下列情形之一的，年度验收考核直接判定为不合格（不通过）：

（1）发生数据安全责任事故或重大信息安全事件（包括但不限于公安工作数据泄露、公民个人信息泄露、图像资料外泄被立案为刑事案件或被公安部点名通报）；

（2）年度验收考核得分低于 80 分；

（3）连续两个考核周期得分均为 80 分（含）以下，且经采购人要求整改后仍不达标的。

年度验收考核不通过的，供应商应按采购人要求限期整改并重新考核；仍不合格的，采购人有权立即终止合同、不支付当年相应费用，并按合同约定追究违约责任。