2、分项报价表

序号	名称	品牌型号	规格	数量	单价	总价	生产厂家
1	非编系统核心网络安全加固（防火墙）	H3C SecPath F1000-AI-75-G	现有一台 H3C SecPath F1000-AI-75 防火墙，新购防火墙和该防火墙配置为双机冗余系统。 1、架构：采用非 X86 多核架构，2U 机架式设备，可热插拔冗余电源，支持扩展 1T HDD、480GB SSD； 2、接口：16 个千兆电接口，4 个千兆光接口，6 个万兆光接口，4 个 Combo 接口，1 个管理接口，2 个 USB 接口，1 个 Console 接口，2 个扩展槽位，2 个接口扩展槽位； 3、性能：吞吐量 15Gbps；并发连接数 500 万，每秒新建连接数（HTTP）12 万； 4、授权：115 个 SSL VPN 用户授权，3 年 AV 防病毒安全特征库升级，3 年 IPS 特征库升级授权，3 年 WAF 特征库升级授权； 5、支持路由、透明、混合模式部署；支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS 等路由协议； 6、支持 BFD 和 NQA 网络协议，支持基于接口状态和路由状态等多种类型的探测机制来及时触发链路切换或主备切换，保障业务连续性； 7、支持 IPsec VPN 智能选路，根据隧道质量调度流量；可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控；SSL VPN 支持页面定制功能特性，包括登录页面、交互信息、提示信息的定制功能； 8、可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；防病毒本地库数量 600 万；支持基于文件协议、邮件协议（SMTP/POP3/iMAP）、共享协议（NFS/SMB）的病毒功能。可基于病毒	1	146000	146000	新华三技术有限公司

			特征进行检测、动作响应、提供报表；支持发现病毒发送的告警信息，支持用户编辑告警内容； 9、支持为 Web 应用提供基于 HTTP 和 HTTPS 的流量防护。对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护；支持至少 4000 种独立 Web 特征的攻击检测和防御特征库； 10、支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便对攻击行为进行取证；支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略；实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御。				
2	用户行为管理系统	深信服 AC-1000-B2500-A4	硬件及性能： ★1、性能：网络层吞吐量 20Gb，应用层吞吐量 9Gb，带宽性能 5Gb，用户数 20000，新建连接数 80000，并发连接数 320 万。 ★2、规格：2U 设备，内存 24G，硬盘 1T，接口 4 个千兆电口+4 个千兆光口+2 个万兆光口，冗余电源。 基本要求： 1、聚焦本单位上网网络行为安全，实现全网资产、身份、行为可视可控，防翻墙管控和审计，提供三年特征库、软件升级和硬件质保服务。 2、支持两台及两台以上设备同时做主机的部署模式。提供技术承诺书并加盖公章。 3、支持账号密码+动态令牌、验证码身份认证，支持通过短信和密码绑定动态令牌。 ★4、设备内置应用识别规则库，支持超过 10000 种以上应用规则数、支持超过 10000 种以上的应用；支持根据标签选择应用，并支持给每个应	2	356000	712000	深信服科技股份有限公司

			用自定义标签：支持根据标签选择一类应用做控制；支持超过 4000 种主流 Saas 应用，对 Saas 应用有默认分类标签，帮助客户统一配置策略（可提供产品手册、公开规格文档、检测报告或产品截图作为佐证）。 ★5、支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；线路空闲值可自定义（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 功能： 1、支持首页显示在线用户、流量分析、行为日志分析、应用流量排名、用户流量排名、资产类型分布、新设备发现趋势、TOP 违规检查项、TOP 违规用户、行为风险分析包括：终端接入、上网安全、系统状态、接入状态； ★2、支持代理控制功能，不允许使用外部 HTTP 代理，不允许使用外部 SOCKS4/5 代理，不允许在 HTTP，SSL 一些的标准端口上使用其他协议（比如在 80 端口上传输非 HTTP 协议数据，在 443 端口上传输非 HTTPS 协议数据等）（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 3、支持管控微信、QQ、钉钉、企业微信、飞书、阿里旺旺等 IM 软件的文件外发行为，不影响其他功能的正常使用，如 IM 发消息等（后附供产品手册、公开规格文档、检测报告或产品截图作为佐证）。 4、支持对上网日志进行大数据分析，包括全网上网态势分析、带宽分析、专线质量分析、未关机检测分析，并可导出报表（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 5、支持 Windows 终端外联行为检查，包括：拨号行为、双网卡行为、有无线网卡行为、连接非法 WIFI、4G 网卡、使用非法网关，对不满足检查要求的终端强制断网，并弹窗提示用户（后附产品手册、公开规格				

			文档、检测报告或产品截图作为佐证）。 6、支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 资料： 1、为保障产品软件开发安全、产品本身无漏洞，所投上网行为管理产品经过国家授权实验室安全监测或安全认证（后附产品手册、公开规格文档、检测报告或产品截图作为佐证。）				
3	网页防火墙系统	深信服 AF-2000-FH3100A	基本要求： ★1、现有两台深信服 AF-2000-FH3100A-3F 防火墙，新购网页防火墙系统适配该两台防火墙。 提供 WAF 安全防护功能、威胁情报功能（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 00000000000000000000 • 2、产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 3、产品支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 4、产品支持云威胁情报网关技术，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 5、产品支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发（后附产品手册、公开规格文档、检测报告或产品截图作为	2	18800	37600	深信服科技股份有限公司

			佐证）。				
4	终端安全管理系统	360 定制	★1、管控中心支持对多类型操作系统同台管理，包括但不限于 Windows 7/Windows 8/Windows 10/ Windows 11/macOS/CentOS，Ubuntu/龙蜥/Mac 操作系统等。支持对国产终端进行统一管理，包括但不限于麒麟 V10/麒麟 V10 SP1/SP2/SP3/麒麟 V11/统信 UOS V20/统信 UOS V25。Windows pc ≥90 点，国产 PC 操作系统≥10 点；Windows sever≥90 点，Linux≥90 点，国产服务器操作系统≥20 点 2、级联部署时，下级中心支持独立导入授权，也支持由一级管控中心对下级管控中心进行授权分配，分配后也可由管理员再次手工调整授权分配数量（后附产品功能截图） 3、产品对外提供标准的 APi 接口，支持第三方获取相关状态和统计数据；支持通过接口给终端下发病毒查杀、主程序升级、病毒库更新等指令。 4、Windows 客户端支持模块化部署，按照管理需求给客户端分配模块，客户端按照已勾选的功能模块进行安装和运行。（后附产品界面截图，并加盖公章） 5、客户端支持自我保护功能，不被恶意结束或结束后自动拉起；支持管理员可设置客户端防卸载，防退出密码，当客户端程序退出或卸载时需要输入正确的密码才可以进行下一步。终端退出/卸载密码支持固定和动态密码两种方式（后附产品功能截图，并加盖公章） ★6、支持终端用户提交故障信息并可上传相关附件，管理员收到信息后可查阅并处理。支持终端用户提交意见反馈信息，管理员收到信息后可查阅并处理（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 7、平台具备全方位、精细化的终端资产自动化盘点采集能力，可全面覆盖各类主机及业务资产维度，支持批量自动化采集软件、进程、开放端口、账户、启动项、计划任务、环境变更、内核模块、运行服务、容器、	1	145000	145000	三六零数字安全科技集团有限公司

			数据库、Web 服务、Web 站点、Web 应用、Web 应用框架、系统安装包、JAR 包、镜像、受信任证书、NPM、龙虾应用等资产。支持从资产角度查看终端安装数量和终端信息，从终端角度查看各类资产数量和详细信息，并支持快速检索和 CSV/Excel 两种导出格式（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 ★8、支持对终端资产是否存在风险进行检测，包括是否存在指定高危端口、是否存在不合规账户、是否存在不合规启动项、计划任务，是否使用未激活系统等。风险支持实时展示以及分类统计（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 9、具备云端样本鉴定能力，有效针对各种病毒文件进行查杀（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 10、产品需支持多引擎查杀技术，至少包括云查杀引擎、大数据特征引擎、人工智能引擎、脚本引擎等 4 个引擎，客户端支持以图形化方式展示各个引擎的信息,以确保产品可适应不同环境（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 11、支持产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 12、支持对扫描文件大小进行设置，同时用户手动扫描时不受管理端的文件大小阈值限制 13、支持从服务端给客户端下发病毒库立即升级指令，升级客户端病毒库。支持终端用户手动更新病毒库版本。支持从服务端管理页面下载病毒库。支持离线更新客户端病毒库。支持从互联网、管理中心、升级服务器进行升级。 14、提供高级持续威胁全景分析：内置 50 个 APT 组织情报信息（包括介绍、MD5、CC 域名、常用漏洞等）、25000+APT IOC 情报库，支持				

			按照已知的 APT 情报对内网进行 APT 攻击痕迹检测，判断终端是否存在已知 APT 攻击行为；支持对存在 APT 漏洞风险的终端进行分类统计（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 15、支持查看服务端下载的补丁文件信息，并可通过服务端页面提供的下载链接下载相关补丁文件。支持管理员配置补丁包含列表、补丁排除列表。终端用户可查看已安装的补丁、已忽略的补丁，可按照 KB 号卸载指定补丁，支持清理补丁安装包，减少对磁盘空间的占用（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 16、支持补丁分发灰度发布功能：当管控中心更新漏洞库时（补丁库），可自动化编排完成补丁库的分发，可将终端分组划分为多个批次，逐步推送补丁（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。 17、提供弹窗防护、软件权限管理、蠕虫病毒防护、隐私防护、主页修复等小工具功能，辅助终端用户提升安全防护能力。提供断网急救箱、流量防火墙、LSP 修复等上网修复工具小工具，解决终端日常运维问题（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）。				
5	统一认证系统	华为定制	1、支持物理机及虚拟机部署，支持异地灾备部署方案（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）； 2、支持自动化编码、用户认证、用户组策略定义、网络统一管理及运维功能； ★3、支持多种身份源对接，如 AD/LDAP、企业微信、钉钉，支持与多个 AD/LDAP 域名服务器同步，支持基于帐号属性映射成本地角色，通过角色进行网络准入授权； 4、支持基于 MAC 和基于 IP 的哑终端认证；支持无感知认证，可在多台认证设备间漫游； 5、第三方网络设备兼容：兼容业界主流厂商网络设备，如思科、华为、	1	196000	196000	华为技术有限公司

			华三等厂商设备； 6、支持双因子认证，包括帐号密码+短信认证等； 7、内置多种终端指纹，支持终端在接入网络时智能识别；支持基于终端识别的进网防仿冒； 8、支持访客自注册，免审批或管理员审批，或接待人通过移动终端审批的访客准入认证。支持内置不小于 5 套默认 Portal 页面； 9、支持可定义 VIP 用户，基于用户和应用双重条件体验保障，满足 VIP 用户视频、语音等关键应用的体验保障（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）； 10、支持终端用户上网时长或流量的限制，达到阈值后用户将提醒用户、限速、强制下线。支持限制最大接入终端数和 Portal 免认证有效时间； 11、支持基于组的策略管理，避免基于 IP 网段的 ACL 规格过载，支持认证点与策略点分离，兼容多厂商设备，兼容 RADIUS 中继认证场景策略随行（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）； ★12、支持用户与 IP 解耦，随时随地接入网络并保持权限一致，并支持与其他厂商设备混合组网，实现业务随行，体验随身，满足权限管控需求的同时，有效保障用户体验（后附产品手册、公开规格文档、检测报告或产品截图作为佐证）； 13、配置 600 个接入认证授权；支持最大认证终端和用于≥20000。				
6	网络管理系统	定制	完善数据中心现有设备监测体系，实现对数据中心基础环境、设备运行状态、软件服务工况、业务信号链路、网络运行状态的实时监测与异常告警；配套提供数字化机房管理、设备物模型库、业务数据采集查询、运维人员管理等功能应用，支撑数据中心智能化运维工作。 1、与现有设备监测系统开展数据对接，将当前监测盲区的三楼交换机纳入监测范围，完成全部在线设备运行状态的数据采集，覆盖中心业务专用设备，以及配套供配电、基础 IT 设备；当设备运行出现异常时，自动	1	285000	285000	郑州中豫视频科技有限公司

			触发告警。 2、对接现有动环监测系统，采集各机房精密空调运行参数，对机房温湿度、漏水监测、视频监控等数据进行实时监测，监测指标一旦超出设定阈值，立即触发告警。 3、实现生产要素数据对接、可视化展示与异常告警，涵盖现有业务数据、节目非编系统业务数据等。 4、搭建设备物理信息资源库：在数据采集端采集设备名称、序列号、上架时间、软硬件版本等信息；在运行管理端提供设备上架、开通等配置能力。搭建运维数据平台，定制适配我台业务的流程化运维管理模块，实现设备上下架、节目上下线、机房巡检等工作的流程化管控。 5、构建专家运维知识库。系统自动沉淀日常告警、故障案例及应急处置方案，支持手动/自动录入故障处置经验持续扩充知识库内容。知识库实现分类管理，当同类故障再次发生时，可通过关键词模糊检索调取历史故障记录与处置方案并可视化展示。 6、建设值班管理子系统。实现值班签到、交接班登记、值班日志、故障事件记录、重要通知管理；支持设备故障信息登记与展示、值班排班管理，并联动专家知识库。 ★7、搭建业务告警统一发布子系统。汇聚被管设备原始告警、监测系统告警，实现告警信息统一分发；支持告警数据综合分析、告警事件与值班管理系统联动，支持通过手机小程序推送设备异常告警消息。 8、完成监测系统综合布线、采集探针部署及综合信息展示大屏实施部署。				
7	存储模块	H3C R4900 G6	产品架构 1、2U 机架式服务器 处理器 2、配置 2 颗 Intel 处理器，单颗主频 2.2GHz，单颗核数 24 核 内存	3	218000	654000	新华三技术有限公司

			3、配置 12 块 32GB DDR5 5600MHz 内存，单节点内存 384GB 系统盘槽位 4、2； 数据盘槽位 5、25； RAID 卡 6、配置 1 块 RAID 卡（4G 缓存，含电容模块） 网卡 1、配置 3 块双端口 25G 网卡（满配 25G 光模块） 2、配置 1 块 4 端口千兆电口网卡 电源及风扇 1、标配冗余电源，模块化风扇 6 个，标准化导轨 服务 1、3 年维保，包含设备安装上架部署服务 授权 1、配置对应存储容量的分布式块存储虚拟化企业版授权 架构 ★1、采用全对称分布式架构和数据冗余技术，随着存储节点数的增加，分布式存储性能和容量也随着线性增长，性能误差小于 10%。 扩容 ★1、支持构建存储集群，集群内节点可在线添加，并且可支持添加硬盘并实现硬盘在线/离线扩容、更换功能，并能实现磁盘的批量扩容，新增磁盘或者节点后，系统可自动实现数据均衡，保障资源的平衡利用。 可靠性 ★1、支持≥3 的多数据副本保护机制，且各副本具有强一致性；支持并行重构丢失的数据；支持在线扩容，支持 PB 级扩展；支持存储和计算				

			分离或融合部署：支持纠删码特性，支持数据重构、重删压缩 块存储 1、支持卷的 IOPS 和带宽同时设置：支持按容量对卷的 IOPS 和带宽同时设置； 2、支持厚配置，可以根据业务需求分配固定的物理存储空间：支持精简配置，可以根据应用实际写需要时才弹性分配相应的物理存储空间； 3、支持卷回收站，在存储卷被删除后，会进入回收站防止误操作，防止数据误删除。支持设置卷回收站的定时清理时间； 4、支持卷克隆、卷拷贝、卷迁移，如从低性能资源池迁移至高性能池。 监控运维 1、支持对 SSD 硬盘进行寿命进行预测，支持故障告警，支持可视化硬件网络拓扑，支持对硬盘故障检测。				
8	业务系统的保障服务	定制	**服务范围及内容** 在招标人管理下，我方负责对非编系统、媒资系统、演播室系统内的硬件设备进行日常巡检、制播保障，对网络安全进行保障，以及所有系统软件、服务器应用软件、终端应用软件的安装部署和维护。 **主要工作和责任包括：** 1. 我方运维团队提供 7×24 小时电话技术支持。对本运维项目范围内中的所有平台系统进行技术维护管理和技术支持，对系统中的核心设备及核心软件的部署、调整和修改，必要时须委托系统集成商派专业工程师来现场实施和指导。 2. 我方制定完善的运维工作规范和管理流程，保证运维人员的各项工作按规范进行； 3. 我方提供运维技术团队人员名单，并为本运维服务项目指定一名技术负责人。当在服务范围内发生驻场运维人员无法解决的故障时，投标人应向招标人提供技术团队的支持，并在规定时间内解决故障；	1	355000	355000	郑州中豫视频科技有限公司

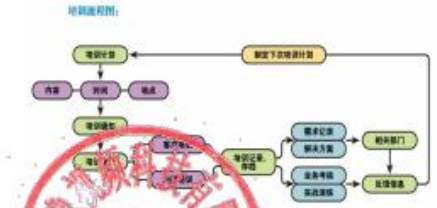
			4.我方按照招标人要求，在重要安全播出保障期或重大活动保障期间，增派技术人员来台加强保障力度，确保所有网络系统稳定运行； 5.我方具有运维技术管理机制，定期对派驻招标人工作的运维人员进行培训和考核，确保运维人员技术水平满足招标人要求； 6.我方在运维人员出现更换、调动时，须提前一个月和招标人申请协商，替换的人员需经过投标人培训、考核，并经招标人管理部门同意后方可更换。 7.我方提供运维人员的各种资料，包括但不限于基础信息，公司信息，无犯罪记录证明，保密协议、岗位安全协议等等。 **派驻现场的运维人员主要工作和责任包括：** 1.运维人员严格按照工作规范，完成机房和系统设备的日常运行巡检监测，及设备的故障处理工作，定期对设备进行安全检查、重启和维护。做好系统的运维日志和巡检报告，定期上报招标人管理部门。确保平台安全运行； 2.运维人员协助招标人使用部门完成应用软件的培训和使用工作； 3.运维人员熟练掌握系统及客户端设备涉及到的技术细节，具有及时判断和处理故障的能力； 4.运维人员接到招标人报修通知后，立即去现场排除系统和设备故障，使系统设备恢复正常； 5.运维人员的工作由招标人领导和管理，遵守河南广播电视台各项系统操作、值班管理等规章制度及网络系统运行管理制度，并完成招标人管理人员安排的日常性工作。 6.运维人员协助招标人管理部门完成网络安全等级保护测评和网络安全整改相关工作。 **网络日常管理运行保障的基本任务** **运维工作时间**				

			新闻网工作时间：早 10:00--晚上 19.30（根据现场需求延长工作时间） 媒资网工作时间：早上 9:00--晚上 17.30（根据现场需求延长工作时间） 工作内容： 每日巡检内容： （1）上午 10:00、下午 14:00 测试节目送演播室流程（一天两次） （2）上午 10:10、下午 14:10 巡检 MAH、MOC 后台 MPC、迁移、合成等服务是否正常（一天两次） （3）10:20 巡检数据库备份是否正常 （4）10:30 巡检 MAH、MOC 后台 nebula 任务流程并处理报错（巡检时间 10-20 分钟一次） （5）10:40 巡检 MOC、MAH 服务和数据库运行是否正常 以下为每半个月一次巡检内容： （1）每半个月巡检虚拟服务器的日志空间、CPU、内存 （2）每半个月巡检演播室视频服务器存储空间 以下为每月一次重启内容： （1）每月重启 MAH、MOC 后台 MPC、迁移、合成服务和服务器 （2）每月重启演播室视频服务器并清理存储空间（重启后测试流程） 以下为每半年一次重启内容： （1）重启所有服务的操作系统 **设备及环境监测保障** 在网络的日常管理维护工作中，及时有效的监测整个系统服务设备的运行环境，才能及时发现网络正常运行过程中潜在的危险以及出现的异常，并能够有针对性的将这些潜在危险或者异常在通过正确分析的基础上采取合理的应对措施。具体职责如下：				

			1、每天监测核心服务器机房的设备运行环境，包括机房 UPS、空调运行状态，以及机柜内设备电源插座的连接情况等，发现问题和隐患及时上报并协助解决； 2、每天监测关键设备的运行状态，发现异常须立即分析原因、解决问题； 3、每天收集、记录环境和设备的运行数据和日志、并加以分析整理汇总； 4、按系统运维规范要求定期重启服务器和关键设备，定期进行核心主备设备的切换演练，充分确保系统安全平稳； **用户权限管理** 用户权限管理是控制网络工作流程和保障系统安全平稳运行的重要技术手段。对共享的网络而言，用户权限管理不仅体现在网络建设时期权限策略的制定上，更渗透于日常管理维护的过程中。在招标人管理人员确认前提下需完成以下工作： 1.用户组织结构、栏目及帐号的新建、添加和删除管理； 2.用户帐号权限赋值管理； 3.用户帐号变更和重置管理； 4.栏目迁移策略新建及变更。 **存储空间管理** 存储空间管理是网络日常管理维护的重要组成部分。需全面考虑到各节目制作的周期、素材和成片的片比、制作和媒资等各子网络的在线存储量，进而对有限的存储空间进行合理的分配和高效的管理。具体管理职责如下： 1.所有非编网系统、融媒内容生产发布平台及媒资系统的用户存储空间大小管理； 2.网络素材盘存储空间大小监控、分析；				

			3.每日媒资节目入库量统计及分析。 **系统关键数据备份** 对与制播网络，数据备份是重要的安全措施，具体工作职责如下： 1.数据库相关配置信息备份； 2.数据库归档日志备份； 3.数据库物理文件定期备份； 4.核心服务器和交换机设备配置文件备份； 5.网络安全设备配置备份； 6.应用软件原始版本及升级包、补丁备份。 7.终端站点系统镜像和软件配置文件备份； 8.网络、设备、软件的变更、改造等其他重要数据备份。 9.定期对备份数据进行整理，当出现系统问题时，能及时恢复备份文件， 10.定期与进行系统更新比较，需要更新时，能及时更新版本。 **运行日志管理** 完善的值班日志和系统周报、工作月报制度的建立和持续，是保证网络管理运行保障质量的重要手段。系统日志有助于网络运行保障经验的积累和总结，有助于网络管理人员的技术交流，有助于设备状态历史数据的收集、调取、整理和分析。 1. 每日记录系统日志，记录系统运行状态（包括：软硬件日志、系统日志和数据库日志等）； 2. 每周记录系统周报，汇总每周系统中的重大问题，布置下周工作重点； 3. 每月记录系统月度工作报告，包括设备使用情况汇总、分析，系统大事概述和现存问题； 4. 将历史日志归档整理。				

			5．定期发送进行日志分析，排除潜在隐患，确保系统稳定运行。 **保障解决以下类别所有问题** 演播室素材主备不同步； 2．MPC 无法处理 H265 视频； 3．70 演播室重新改造系统数据库迁移稿件锁定无法打开； 4．MPC 无法处理繁体字； 5．非编采集功能无法使用； 6．出库审核统计时长异常网页上传； 7．无法大批量编辑元数据编目中弹窗无法拖拽； 8．资源详情页中相关推荐存在打回节目； 9．大库中资源编目人显示不对入库时间改为审核发布时间媒资无法上传； 10．配合播出调整接口清理素材脱管文件。 **运行保障制度管理** 规范制度对整个系统的运行起到关键的指导作用，相关规范的制度内容如下： **技术文档管理** 所提交文档包含但不仅限于以下内容： 将河南广播电视台，投标人、第三方厂家提供的电子文档资料，存放在指定的目录中，规范文档的命名格式和索引文件，便于日后查询。 规范化撰写存档符合河南广播电视集团制播网维护的规范制度。 规范化撰写存档系统中所有应用软件的操作文档。 规范化撰写存档系统中所有站点、服务器的安装、配置文档 1)客户端运行保障规范 2)存储系统运行保障规范 3)网络系统运行保障规范				

			4)数据库系统运行保障规范 5)防病毒运行规范 6)日志交接管理规范 7)值班人员日常规范 **报告管理** 所提交报告包含但不仅限于以下内容： 按具体的工作岗位撰写的存档日报、周报，月报，季度总结 据客户需求整理的汇总文件 河南广播电视集团和投标人的书面总结和报告以及各种沟通文件 异常问题的分析及解决报告 培训管理  **运行保障培训内容包括：** 组织学习河南广播电视集团业务规范； 组织学习投标人的应用系统操作规范； 组织学习第三方厂家提供的操作规范 组织学习讨论日常维护过程中经验； 技术交流与培训。 系统运行保障人员通过各类会议、工作计划、工作汇报等形式，循序渐进地有针对性地就运行保障的工作内容、系统的最新需求、系统存在的问题等状况进行长期的内外部交流和沟通，确保畅通的交流渠道加				

			速问题的反映和解决过程。其中技术交流和运行经验分享每月至少开展两次，并提供相应的材料。 **紧急事件的应急措施** 处理紧急事件的宗旨 （1）尽快将节目生产恢复到正常状态 （2）将事件造成的损失降到最低 （3）如实、快速的向招标人和厂家汇报事件处理的进度 （4）快速、准确的保留事件的日志 紧急事件处理流程  （1）紧急事件出现后，运行保障项目经理在最短时间到达现场协调各项工作，并由现场技术力量最强的运行保障人员分析、检测、诊断； （2）确认问题后，在最短的时间内进行处理； （3）应用软件问题，迅速寻求公司开发人员技术支持； （4）设备硬件问题，寻求网络工程部以及第三方厂家技术支持； （5）解决完毕后，紧急事件记录、分析、撰写故障报告； （6）长期观察排除类似隐患； **运维保障人员具体职责** 运维保障人员须在招标人管理部门的领导下开展工作，对制播网络的硬件设备调整、软件参数配置与修改，应用数据修改等变动报批招标人管理部门领导审批。				

			系统运行保障 职责：在线存储系统、近线存储系统、数据库服务器硬件和操作系统、数据库软件、网络系统等的运行管理。包括：系统监控、故障报警、故障诊断、系统恢复、数据备份、日志分析、常规维护等业务。 **管理维护** 职责：域控服务器、应用服务器、调度服务器、迁移服务器、合成服务器、播出服务器、播控工作站、非编工作站以及服务器相关软件的日常运行和保障工作。包括：系统监控、故障报警、故障诊断、日志分析、系统恢复等业务。 **演播室播出系统保障** 职责：负责演播室播出子系统的日常流程测试，应用软件、工作站设备的正常运行。保证日常节目顺利制作和播出。参与招标人技术部门和节目部门的应急演练，熟悉应急方案。非正常情况下，提出处理措施并尽快恢复设备正常运行，或者采取应急预案，保证节目安全播出。 **软件版本的测试、整理** 职责：对系统中所应用软件的版本进行整理和软件功能测试，以及软件系统在应用中出现的问题汇总。并配合其他系统与本系统相关接口的测试和故障排查。 **病毒防疫** 职责：按照河南广播电视集团相关部门规定对系统安装相应杀毒软件，保障系统内部不受病毒侵犯。 **第三方操作系统的补丁完善** 职责：应根据微软操作系统补丁更新情况及第三方应用软件如数据库等补丁更新情况，负责及时提供经过测试后不影响河南广播电视集团制播网络系统正常运行的微软操作系统或其它第三方应用软件的补丁版本。				

			与招标人技术部门管理人员协商提交补丁更新申请、升级风险、重要度和操作步骤等方案，待招标人负责人确认可以实施后，协助在系统中更新系统补丁。 **应用软件补丁升级** 职责：如确定应用软件出现漏洞或 BUG，须及时向系统集成商提出修改申请，待集成商的软件补丁发布时，须配合升级测试，完善软件功能。 如确定软件出现 BUG 需要进行补丁升级时，运行保障人员需与招标人相关部门人员协商提交补丁更新申请和操作步骤等方案，待招标人技术部门负责人确认后方可实施更新补丁。 在确保不影响正式系统业务的情况下，招标人可先小范围进行补丁测试，测试正常后再进行全面的系统更新。 **系统培训** 职责：协助河南广播电视集团相关部门，负责对相关技术人员和使用人员进行必要的系统使用培训。 **硬件维护** 职责：负责网络系统硬件以及配件检查操作。 负责检查网络系统内硬件以及配件是否工作正常，如确定系统中设备出现硬件故障需要更换时，运行保障人员需要与招标人相关部门人员说明情况，待确认后更换硬件。 **日志记录存档** 职责：运维人员需要定期完成完整的日志记录并存档，定期（如：周或月）递交招标人相关部门一份。 **提交运行保障报告** 职责：系统运行工作组负责人负责起草所有提交河南广播电视台技术管理部门的报告，同时负责协调运行和管理工作，包括系统软件检查、				

			软件系统维护：数据定期整理等；并向相关部门提交报告，并协助河南广播电视台做相关数据统计分析工作。 **应急演练** 职责：定期进行系统内主要服务器及网络设备主、备机倒换运行的应急演练，制订详细的应急文档及可行性报告，准备详细的实施方案以及操作存在的风险性上报招标人管理部门，经批准后实施。 **应急恢复** 职责：建立必要的快速故障和系统应急恢复手段、措施及相应的操作手册。对关键的设备应立刻响应，判断出故障原因后快速恢复。 对于一般性故障应及时判明故障原因，提出解决方案，在故障发生后一天至两天内解决问题。 对于严重故障，具备备份设备的，应立刻启动备用设备确保系统运行正常，在确定问题原因后三日内解决问题，无备份设备应采取临时措施，确保系统运行正常。如有必要，需联系系统集成商委派资深人员到场解决。 **网络安全等级测评和整改** 职责：根据国家网络安全相关法律和法规，以及招标人网络安全管理方面的相关要求，专业新闻高清网须定期完成网络安全等级保护三级的测评和整改工作。运维人员在测评和整改工作期间，须积极配合招标人技术管理人员，对测评需要的网络构架信息、设备信息、操作系统和应用软件的配置、系统运行流程、系统运行日志等数据收集工作提供技术支持，并对测评要求整改的项目提供技术实施，必要时应向投标人公司请求技术协助，保障招标人网络测评和整改工作的顺利完成， 对于国家、省、市网络安全管理部门发布的网络安全相关检查、整改工作要求，须积极配合招标人技术管理人员按照检查和整改方案实施。 **配合其他厂商的工作**				

			职责：按照招标人管理部门的需求配合其他厂商进行正常运维、故障排除、测试和调优工作。 **时间安排和人员配备** **时间安排** 投标人派驻现场的运维工程师，须根据招标人的工作时间安排，向该网络平台区域及演播区域提供一年 365 天、7×24 小时（根据直播节目需要）的现场、电话、网络等方式的技术保障支持。每天现场保障最少一人在岗，每周每人 40 小时的在岗时长。 **人员配备** 我方保证在招标人正常工作时间内不少于一名系统运行维护人员在现场进行驻场技术保障，同时投标人还应向招标人提供运维团队的技术支持，并指定一名技术负责人。当招标人所要求的服务项目有重大调整、或发生现场人员无法解决的故障时，投标人应在服务范围内向招标人提供团队技术支持。  **投标人人员要求** 我方为招标人提供德、才、能兼备的网络技术运维人员，并接受招标人对其工作上的管理。该人员必需满足以下技能要求： （1）具备过硬的政治素治，遵守国家法规规定； （2）具备较强的工作责任心和良好的服务态度；				

			（3）严格遵守招标人的信息保密制度； （4）能独立完成非编制作网络及设备各种故障的处理； （5）能独立对各种计算机网络应用和 IT 设备的故障进行处理； （6）能熟练掌握非编制作网各种软件、媒资系统软件及各种通用软件的使用方法； （7）如因个人原因，投标人运维人员在正常工作日需请假的，需向招标人提前提出申请，由投标人安排其他运维人员在招标人现场进行保障； （8）招标人对我方提供的网络技术人员可进行为期两个月的试用，对试用不满意的，我方更换人员；我方如因工作需要等原因更换现场维修人员，提前 1 个月通知招标人。 （9）在招标人有重大活动和重要保证期内，投标人应按招标人提出的合理要求对网络系统加强保障，增配现场运行保障人员。为保证节目制作、播出安全，投标人网络技术人员应固定，尽量减少人员的更换。				
合计人民币：贰佰伍拾叁万零陆佰元整（大写）：¥：2530600.00 元（小写）							

说明：1、如不提供分项报价将视为非实质性响应招标文件。

2、本表的合计价格应与河南省公共资源交易中心所提供《开标一览表》与《投标报价表》的投标总价一致。

3、本表适用于本项目所有包段。

投标人名称（电子公章）：郑州中豫视频科技有限公司

法定代表人或被授权人（签字）：史淑红

日期： 2026 年 11 月 17 日