采购需求

一、商务要求

序号	审查因素	审查标准
1	※投标文件签署、盖章	投标文件按招标文件要求签署、盖章的
2	※投标文件格式	符合招标文件中提供的投标文件格式
3	※报价唯一	只能有一个有效报价
4	※投标报价	报价未超过招标文件中规定的预算金额或者最高限价的
5	※投标内容	符合第二章“投标人须知前附表”第 1.2.4 项规定
6	※售后（维护）服务期限	符合第二章“投标人须知前附表”第 1.2.6 项规定
7	※服务地点	符合第二章“投标人须知前附表”第 1.2.7 项规定
8	※质量标准	符合第二章“投标人须知前附表”第 1.2.9 项规定
9	※投标有效期	符合第二章“投标人须知前附表”第 3.6.1 项规定
10	售后服务方案	提供服务期内服务计划、服务内容（包括完善的售后服务体系、完备的服务团队、故障响应时间、巡检）
11	培训方案	提供培训内容、培训计划、培训方案
12	服务承诺	提供履职尽责承诺，具有保证技术措施落实到位的承诺和落实不到位的处理承诺，其中包括各关键岗位人员（负责人及相关技术人员等）的在岗、更换等履职尽责承诺。

二、技术要求

包 1：互联网安全加固

1、DNS 安全防护系统（1 台）

指标项	指标要求
配置项要求	★ 软硬件一体化设计，千兆电接口≥6 个，支持接口扩展，每秒查询率≥150000 次，内置存储空间≥1T，冗余电源。系统配置权威域管理、递归域管理、DNS 防火墙、告警通知、网络工具、用户角色管理、服务集群管理、操作日志、DNS 日志等功能模块。
总体要求	支持纯 IPv6、纯 IPv4 及 IPv6/IPv4 双栈解析，满足国家 IPv6 升级改造要求。
DNS 转发要	支持 DNS 转发，包括全局转发、基于线路的转发、基于域名的转发，转发服

求	务器可设置多个，支持定时转发策略的关停与开启；支持同时迭代和转发模式的递归域名解析，包括但不限于第一次转发、强制转发、智能转发、递归失败后转发等。
记录要求	支持双栈模式下 IPv4 记录和 IPv6 记录过滤功能，有效减少无效查询和数据传输；支持指定递归域名的 AAAA 解析内容过滤，只返回指定域名的 A 记录过滤 AAAA 记录，同时其他域名的 AAAA 解析不受影响。
安全要求	内置下一代防火墙模块，支持防 DoS/DDoS 攻击模块，内置安全规则，支持自定义基于 IPv4/IPv6 地址的防火墙规则；支持单 IP 地址并发解析速率限制，支持包括可用最大数据内存、TCP 并发连接数量、递归查询请求超时、缓存最大占用内存百分比等参数在内的资源设置以保证设备的资源安全。
	支持高性能模式和 Servfail 防护功能，支持源 IP 黑白名单功能，可以拒绝指定 IP 查询及访问，可以允许指定 IP 访问和管理智能 DNS 系统。
	★ 配置 DNS 防火墙模块，内置病毒、木马、网络钓鱼以及广告等恶意域名数据库，域名库数量不少于 80 万条；支持威胁域名数据库在线管理、自动更新，支持自定义设置拦截响应，支持 DNS 防火墙日志及威胁主机定位与导出功能。（提供证明截图并加盖原厂公章）。
	★ 支持与态势感知联动实现对“挖矿”域名实时进行拦截，提供威胁域名数据库 API 接口文档。（提供联动证明效果截图及并加盖原厂公章）
监控要求	配置智能监控告警模块，支持自定义监控类别与监控阈值，监控类别包括但不限于 CPU 利用率、内存利用率、存储空间、系统负载、CPU 温度、解析成功率率等，支持多种告警方式，包括邮件、短信、微信。
功能要求	支持 DNS 负载均衡功能，支持递归解析链路监视功能，在被监视的链路发生故障时切换至其它正常的链路进行域名查询，保证客户端解析请求不受影响。
	★ 支持特权模式设定，只有进入特权模式才可以对设备进行“写”操作；支持回收站功能，支持恢复被删除的集群、域、线路、记录（提供截图并加盖原厂公章）。
	支持远程协助功能，无需在出口网关上对互联网开放管理端口便可协助用户进行安全的远程技术服务；支持 IAM 基础服务控制台集中管理。
日志报表要求	★ 提供内网主机事件报表分析模块;支持威胁事件主机统计，支持根据时间段、线路、内网主机、威胁名称、恶意域名拦截时间进行排名，支持威胁主机导出。支持安全事件报表分析、支持根据时间段、请求方、威胁类型查询统计，支持根据威胁严重级别进行统计，支持恶意地址、威胁事件角度进行分析。支持非法域名类型的安全事件报表分析、支持根据时间段、请求方、威胁类型查询统计，支持 DNS 查询趋势、威胁分类及 TOP 威胁域名排行及导出功能（提供截图并加盖原厂公章）。
	支持 DNS 防火墙安全日志分析，支持登陆日志、访问日志、操作日志、系统日志、API 日志等 DNS 全面日志，支持基于查询次数与拦截次数、威胁类型、TOP 受威胁主机、威胁域名 TOP 排行、来源线路统计、域名库统计等数据统计。
	具有丰富的 DNS 解析日志及统计报告，所有节点 DNS 解析实时展示和统计，支持图形化展示，可显示基于世界与中国地理位置的来源地区分析、解析量分析、权威域名分析、递归域名分析、IP 来源分析、解析线路分析、记录类型分析。

	支持在系统首页集中通过饼图、柱状图实时展现服务设备访问数据，包括QPS、Top 域名、Top IP 、解析记录统计等。
其他要求	为保障产品质量，产品厂商需通过高新技术企业认证，投标时提供证明文件。
售后服务	提供 3 年特征库升级服务，提供 3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

2、外网综合安全网关（1 台）

技术指标	具体要求
基本要求	1. 硬件参数：配置独立的 1 个 CON 口，2 个 USB3.0 口，1 个 MGT 口,1 个 HA 口；配置≥8 个千兆 SFP 光口，≥8 个千兆电口，≥4 个万兆接口。可选配 480G/960G/1.92T/3.86T SSD 硬盘；配置冗余电源； 2. 性能参数：吞吐量≥40Gbps，最大并发连接数≥1000 万；每秒新建会话≥31 万；IPS 吞吐量≥17.5Gbps；最大 IPsec VPN 隧道数≥20000； 3. 配置三年入侵防御库升级服务。
功能要求	1. 支持透明桥旁挂部署模式下的基于 vlan 标签改写替换功能以实现二层引流，支持 vlan 和 vlan 之间流量的安全过滤。 2. 系统支持 Flood 防护阈值学习功能，通过统计各种正常业务流量数据，进行检测阈值的智能学习，得到各种攻击流量类型对应的合理阈值，为攻击检测阈值提供合理参考。 3. 支持零信任功能，支持 SPA 单包认证功能。具备独立于防火墙策略之外的零信任安全策略，且支持禁用和启用，并且支持结合 AV\IPS 等安全防护。支持应用发布，客户端登录成功后，支持推送客户端被授权的应用清单。 4. 入侵防御特征库支持网络实时更新；支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等。 5. 支持 IPv6 的静态路由、策略路由、ISIS、RIPng,OSPFV3、BGP4+;支持 NAT 及 ALG，支持 NAT444，NAT64、DS-Lite，Full-Cone-NAT 等地址转换技术。 6. 为了避免 IOT 设备被攻陷所造成的安全隐患，要求产品可以实现分析流经设备的流量，识别视频监控专网中的 IPC 和 NVR 等网络视频监控设备，并对识别出的设备进行实时监控，根据自定义配置对出现非法行为的网络视频监控设备进行阻断操作。 7. 产品必须支持全功能 CLI（SSH、TELNET、CONSOLE 等方式）命令配置，以方便快速进行脚本操作和故障调试，且 CLI 配置必须支持中文输入。 8. ★ 支持策略助手功能快速生成安全策略，通过策略助手能够提取命中指定策略 ID 的流量作为数据流量分析源，生成服务并且根据管理员设置的替换规则，聚合规则优化流量数据，最后自动生成符合管理员期望的安全策略规则，方便管理员维护；（提供第三方机构测试报告，并加盖厂商公章） 9. 支持双病毒检测引擎。支持至少五层解压的压缩病毒文件的扫描，病毒库支持网络实时更新。 10. 支持基于源\目的 IP\域名的具体流量提供 DNS 代理能力，支持与 360 等安全 DNS 直接对接，使用 DOH 协议传输 DNS 报文。 11. ★ 为满足后续软件扩展能力，要求所有产品提供容器化服务，支持第三方 Docker 镜像版本的导入和更新，支持第三方 Docker 运行信息的查看、停止、重启操作；为保证产品系统稳定性，要求产品支持至少 2 个系统软件并存，在 web 界面

	就能直接操作系统版本的快速回滚，设备支持记录 10 个以上的历史配置文件，以便遇到故障后快速进行配置的回滚。
其他要求	★ 投标产品具备中国信息安全测评中心颁发的信息技术产品安全测评证书。
售后服务	★提供 3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

3、零信任移动应用网关控制中心（1 台）

技术指标	具体要求
性能要求	最大并发用户数（个）≥2000，新建用户数（个/秒）-本地认证≥90，新建用户数（个/秒）-外部认证（如 LDAP）≥60。
硬件要求	零信任控制中心和安全代理网关，采用部署分离式部署，硬件参数：1U，内存大小≥16G，硬盘容量≥128G SSD，接口：千兆电口≥6 个、千兆光口 SFP≥2 个。提供不少于 500 点用户接入授权，不少于 500 点安全工作空间授权，配套千兆多模光模块 2 个和光纤线 2 条。
虚拟 IP	支持以虚拟 IP 方式，访问真实的业务系统，以配合其他对 IP 有要求的安全设备工作，以及便于流量分析类设备进行流量分析。
手机 SDK	★ 支持 iOS、安卓手机 APP 集成零信任 SDK，从而实现安全接入、数据安全沙箱等功能，避免单独安装零信任手机客户端，支持通过控制台上传 Android、iOS 原包应用进行自动封装。（需提供第三方检测机构出具的检测报告证明）
应用封装	支持通过控制台上传 Android、iOS 原包应用进行自动封装，使 APP 具备零信任接入能力，支持封装后从控制中下载的封装后和封装前的安装包；支持应用封装列表展示，支持应用详情展示，支持基于已经封装的应用覆盖上传新的安装包，支持主应用自动封装和子应用自动封装。
客户端应用商店	1、支持移动端零信任客户端内置应用商店，应用商店可以展示分发给用户的全部 APP 应用及 H5 应用，并对待更新的应用单独列出。 2、支持直接在应用商店中下载、安装并打开应用； 3、支持在应用详情中查看当前应用的安全权限，包括但不限于网络访问限制、文本复制权限、内容分享至个人应用权限、读取个人应用文件权限、接受个人应用分享权限、水印等。
移动应用发布	1、支持在控制台对原包应用进行自动封装并发布给终端用户； 2、支持在控制台上传已集成零信任 SDK 的生态应用，并发布给终端用户； 3、支持在控制台配置 H5 应用并发布给终端用户； 4、支持上传应用原包，不进行处理直接发布给用户。
终端数据保护	为保障应用数据安全性，应支持针对不同应用配置数据安全策略，包括但不限于：文件读取控制、内容分享控制、数据拷贝控制、截屏控制、应用水印、应用锁等。
	★ 支持针对发布的 WEB 应用开启 WEB 水印功能，水印内容是否包括:用户名+当前年月日（需提供第三方检测机构出具的检测报告证明）。
	支持对工作空间添加屏幕水印；支持为工作空间配置禁止截屏策略；支持工作空间内允许截屏时，或对工作空间拍照时，截图和照片带有水印信息。
代理访问	★ 支持基于 TCP、UDP、ICMP 协议代理访问业务资源，支持发布 IP、IP 范围、IP 段、具体域名及通配符域名形式的服务器地址；能够支持同一个资源发布多个服务器地址。（需提供第三方检测机构出具的检测报告证明）
安全审计	应支持将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员

	快速审计定位。用户安全日志包括但不限于：帐号安全、中间人攻击、SPA 安全、cookie 劫持等。
业务访问审计	支持对 WEB 应用通过无客户端智能脚本技术实现业务访问审计，非录屏、非远程桌面、非堡垒机方式，并支持将审计数据传递至日志中心或分析中心，还原出页面内容、鼠标移动、用户操作等用户访问业务的操作过程视频。
终端环境排查	支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复；支持客户端应用访问诊断，输入应用地址后自动检测应用连通性；支持客户端自助日志收集。
文件加密	★ 支持以文件为单位，对工作应用产生的数据进行加密保存；文件加密支持“一文一密”即每个文件独立密钥，以确保沙箱组件被卸载、模块驱动被摘除的情况下，终端用户仍无法明文取出文件。（需提供第三方检测机构出具的检测报告证明）
其他要求	1、要求所投产品符合 CCRC-TR-119-2022《零信任安全网关技术要求和测试评价方法》(增强级)认证要求；（提供证书复印件加盖厂商公章证明）
售后服务	★提供提供 3 年特征库升级，3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

4、零信任移动应用网关代理网关（1 台）

技术指标	具体要求
性能要求	最大理论加密流量（Mbps）≥300，最大理论并发用户数≥3000，最大理论 https 并发连接数（个）≥30000，理论 https 新建连接数（个/秒）≥400。
硬件规格要求	零信任安全代理网关硬件配置，高度 1U，内存大小≥16G，硬盘容量≥128G SSD，接口：千兆电口≥6 个、千兆光口 SFP≥2 个。配套千兆多模光模块 2 个和光纤线 2 条。
部署架构	零信任控制中心和安全代理网关，应支持部署分离式部署，以实现控制面与执行面分离，提高系统安全性，控制中心与代理网关为同一品牌。
网络部署	为了满足灵活部署的要求，代理网关应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口。为了保护设备的安全，可支持默认限制所有 IP 通过 WAN 口访问系统，支持通过配置 IP 白名单的方式来放通 WAN 口接入的特殊需求。
端口聚合	为充分利用设备的网络性能，代理网关部署时支持配置聚合网口，并支持将聚合网口作为代理网关的网络部署 IP。聚合网口支持通过哈希或 802.3ad 等标准对闲置网口进行网口绑定，支持通过 ARP 探测机制对聚合网口进行健康检查。
支持全面的日志记录	★ 支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等。（提供产品功能截图证明，加盖原厂公章）
流量镜像	★ 支持将用户访问零信任系统的 WEB 资源访问流量解密后镜像给外部网络流量分析系统，如态势感知等设备，以完善系统的用户行为审计溯源能力，提升设备自身的安全性。（提供产品功能截图证明，加盖原厂公章）
管理员分级分权	★ 支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权。管理组支持按控制台模块分配权限，支持对模块配置[只读]、[完全控制]两种权限。（提供产品功能截图证明，加盖原厂公章）
设备安全	支持防机器人输入，提供强安全性的点击图像校验码机制，图形校验码支持中文和英

	文。
	★ 支持 API 接口爆破检查，API 接口越权调用，API 接口扫描，API Web Shell 攻击。（提供产品功能截图证明，加盖原厂公章）
其他要求	要求所投产品厂商具备中国网络安全审查技术与认证中心颁发的《信息系统安全运维服务资质（一级）》（提供证书复印件加盖厂商公章）
服务要求	★提供提供 3 年特征库升级，3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

5、蜜罐系统（1 台）

指标项	指标要求
硬件性能要求	2U 标准机架式，交流冗余电源，2 个 USB 接口，1 个 RJ45 串口，2 个千兆管理口，配置≥4 个千兆电口，≥3 个接口扩展槽（2SFP+/4SFP/4GE），≥256G 固态硬盘，≥1T*2 机械硬盘，面板带液晶显示屏，≥50 个虚拟蜜罐授权。
安全性	蜜网部署期间可通过 Vlan 隔离实现真实内网物理隔离。 不开放蜜罐访问外网与内网权限，切断蜜罐到其他网络访问路径，防止攻击逃逸。
仿真能力	支持高交互蜜罐，并可同时启用：“ftp、ssh、telnet、smtp、dns、wordpress、fanwei、tongda、thinkphp、nginx、NTP、cldap、openVPN、mssql、gtp、mysql、svn、coap、redis、weblogic、tomcat、struts2、jboss、elaseticsearch、memcache、mongoDB、icspot、IOT、Blackhole、jenkins、zabbix”等，以上服务须为真实应用服务，能够正常交互，欺骗攻击者。 ★ 支持工控蜜罐类型的仿真，至少支持工控服务类：Bacnet，S7Comm，Modbus，SNMP，IPMI，EN/IP 等。要求提供功能截图证明并加盖原厂公章 支持 IOT 蜜罐类型的仿真，至少支持 IOT 服务类：GTP 等。 系统默认支持 CVE 等漏洞的内置，预置漏洞类型包含 web 漏洞、应用系统漏洞、数据库漏洞等，预置漏洞数量不低于 45 种。
攻击诱捕	★ 针对客户内部各种复杂多变的网络环境，支持提供二层交换机跨网段部署与三层跨路由部署的方式，实现一台设备，多网段仿真蜜罐的部署，极大提高黑客攻击蜜罐的概率。要求提供功能截图证明并加盖原厂公章 ★ 可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统，真正有效消耗攻击资源，并直接保护真实资产。要求提供功能截图证明并加盖原厂公章
攻击感知	★ 支持攻击诱捕的场景分析，至少包括：WEB 狩猎、物联网狩猎、业务专项狩猎、基础服务狩猎、文件共享狩猎、远程登录狩猎、工业控制系统狩猎、DNS 狩猎、数据库狩猎、邮件狩猎等 10 种攻击感知的狩猎诱捕场景。要求提供功能截图证明并加盖原厂公章 支持对攻击行为的三个维度的分析：狩猎事件、攻击源画像、失陷主机。分别从事件、攻击者、失陷主机的视角进行分析画像。 支持基于攻击日志的行为分析，至少包括：暴力破解、命令执行、代理转发、漏洞利用、蜜罐环境对抗、扫描探测、攻击工具利用、数据库操作、横向移动、恶意邮件、DoS 攻击、外联 URL、文件泄露、恶意文件加载、尝试登录、WEB 请求等 16 种攻击类型分析。 支持攻击长镜头告警分析：可对攻击者的整个攻击过程进行长镜头回放。

	参考 MITRE ATT&CK，采用多种取证技术手段，还原黑客攻击入侵蜜罐的过程，形成黑客攻击链，攻击链检测包含：侦查、工具制作、投送、攻击渗透、安装工具、命令控制、恶意活动等攻击入侵过程。
攻击反制	支持反制技术，可对攻击进行精准有效的反制，支持浏览器漏洞反制技术，获取攻击者信息。
攻击者溯源	设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型。 位置信息溯源至少包括：真实攻击 IP（攻击者拨 VPN 也可获得真实攻击 IP）、代理转发前的 IP 地址、IP 地理位置。 支持自适应溯源攻击者的“黑客社交画像”信息，包括社交账号、手机号、昵称、用户 ID、头像等信息，支持多种黑客社交画像，并支持动态展示。
狩猎监控可视化	支持展示整体狩猎诱捕态势，呈现蜜罐监控概况，包含：高危攻击者数量、失陷主机数量等；威胁狩猎的诱捕结果，按照业务狩猎分类、诱捕结果的分类及各类型的数量。点击每种类型数字和事件名称，均可进行下钻跳转。 支持大屏展示功能，可视化呈现监测数据，实时展示最新监测结果，包括：狩猎事件 TOP5、攻击源 TOP5、狩猎事件趋势图、攻击源低于统计趋势图、最新攻击者实时呈现等，展示数据的时间维度包括：最近一周、最近一个月、全部。大屏数据自动更新。
响应处置	支持和安全设备进行对接，实现攻击黑客访问阻断。
其他要求	产品具有中国信通院颁发的《网络攻击溯源能力检验证书》，提供有效证书的厂商盖章复印件。
	生产厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件。
	生产厂商获得 ISO 22301 业务连续性管理体系认证证书，提供有效证书的厂商盖章复印件。
售后服务	★提供 3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

6、防病毒网关系统（1 台）

指标项	指标要求
基础要求	2U 机架式，内存≥64G，硬盘容量≥1T；千兆电口不低于 2 个，万兆光口不低于 6 个，网络层吞吐率≥15Gbps，要求不低于 2 个闲置扩展槽。
	要求提供防病毒、勒索软件防护安全模块、IPS（含虚拟补丁）模块；提供 3 年免费升级服务（病毒库、病毒引擎、软件版本）。
支持协议	支持不少于 100 种协议，包括不限于 HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC 等
病毒防护	★ 能够支持 SMBv1/SMBv2/SMBv3 文件共享协议的病毒检测与查杀（提供截图并加盖厂商公章）。
	防病毒文件扫描客户可自定义大小，最大可支持 2G。
	★ 需要具备在网络边界的挖矿检测和拦截能力，在界面上能展示矿池协议、挖矿事件的统计数据（提供截图并加盖原厂商公章）。
高级威胁防护	能通过 CVE 编号搜索对应的防护规则，在网络层面对漏洞攻击进行阻断，规则数量不少于 15000 条。
	★ 能对识别到的扫描设备进行流量处理，处理措施包括但不限于阻止全部、

	阻止中高危 CVE 漏洞（提供截图并加盖原厂商公章）。
可靠性	支持自动/手动硬件 BYPASS 功能。
	★ 支持一键 bypass 功能（提供截图并加盖原厂商公章）。
联动能力	★支持与医院现有服务器安全产品、高级威胁发现系统等产品实现联动对接并同步本地威胁情报以及统一的规则库更新管理（提供联动对接证明或对接承诺并加盖厂商公章）。
其他要求	非防火墙产品，须具备防病毒网关类的销售许可证或网专检测证书（增强级）。
	产品制造厂商具有中国网络安全审查技术与认证中心认证的信息安全服务资质证书-软件安全开发类一级资质。
	产品产品厂商具备 ITSS 信息技术服务运行维护服务能力成熟度等级二级及以上资质。
售后服务	提供 3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。

包 2：OA 协同办公系统

一、采购需求

序号	采购内容	采购数量
1	国家心血管病中心华中分中心协同办公系统建设	1 套
2	阜外华中心血管病医院协同办公系统维保服务	3 年
3	阜外华中心血管病医院协同办公系统版本升级	1 次
4	用户数增加	200 个

二、参数要求

1.国家心血管病中心华中分中心协同办公系统建设

1.1 组织人事管理

根据分中心的组织架构，建立符合分中心需求的多维度组织架构，同时便于组织架构的维护和调整，支持建立临时工作小组。

1、基础管理：包含行政区域、办公地点、职务岗位、职称、学历、用工性质等人事管理基本信息维护。

2、组织架构管理：维护分中心行政组织结构和人员，支持多维组织、虚拟组织等，支持共享群组等功能，组织人员信息可以批量调整维护。

3、账户中心：维护设置密码策略、登录方式和网段策略，可以添加第三方校验方式，用户个人隐私策略。

4、权限管理：支持组织分权和功能分权，可支持多级组织架构体系的权限设定，支持灵活的权限调整，可以进行权限转移、复制、删除，便于组织架构的变动。

5、矩阵管理：支持维护系统矩阵和自定义矩阵，矩阵可作为流程节点操作者。

1.2 门户管理

建立分中心内部的信息发布和共享的平台，实现信息通过授权可以多点发布，集中展现。

1、门户自定义：支持门户的个性化自定义，具备丰富的元素库、统一的样式库，满足不同

角色人员的使用习惯。
2、门户权限控制：支持严谨的权限控制体系，包括门户级权限、元素级权限和内容级权限，保证构建的信息门户及信息板块可独立提供给相应使用者查阅。
3、门户信息管理：支持统一的信息发布，支持信息集中发布审核、信息分级栏目定制、信息统一检索等。
4、门户标准管理：支持统一的界面标准、统一的权限标准，支持门户的分级分权管理。
5、多层级门户管理：支持多级、多层门户的构建，可以满足多级信息的发布。

1.3 流程管理

建立符合分中心具体需求的工作流程管控平台，实现分中心流程管理规范化和标准化。
1、流程引擎：自带自主开发的流程引擎，支持内部各类流程的设定，不受第三方限制。
2、流程自定义：支持流程自定义功能，支持子流程，支持复杂工作流的设置。支持对工作流的组成因素包括流程完成需要的阶段、每个阶段的负责人、流转条件，直至相对底层的表单和字段进行自定义，使得工作流的定义完全与实际需求相符合。
3、图形化流程设计：支持流程的图形化设计，可以拖拽的图形化界面方式实现流程的定制和编辑，同时要求流程的定制与组织架构无缝结合，在流程图定制操作上要求具有较强的可用性和便利性。
4、流程维护：支持维护人员随时对现有流程的字段、审批节点、操作者进行调整，在不影响历史数据的前提下，快速响应组织与业务需求的变更。
5、打印模板：支持无水印打印模板，根据不同的工作流表单定制相应打印模板，确保工作流表单可按指定样式进行打印。
6、流程提醒：支持丰富的消息提醒机制，提供流程审批超时提醒，审批通过提醒，退回提醒等功能，提醒方式包括流程提醒、邮件提醒、即时消息提醒等多种提醒方式，提升流程处理效率。
7、流程版本控制：支持流程多版本，不会因为流程版本的更新导致原流程中的申请单出现问题。
8、流程导入：支持通过 EXCEL 可以对流程表单、字段、流程审批环节进行定义，通过一键导入方式自动将 EXCEL 中的流程表单、流程图、流程字段批量同步到系统，无需进行二次维护即可快速创建流程。
9、流程仿真测试：支持对未发布的流程和规则进行自动检查校验和模拟测试。
10、流程自动触发：支持根据设定时间、根据事件（如新建文档、系统流程审批等）自动触发启动工作流。

1.4 公文管理

建立分中心的公文管理平台，实现公文审批的无纸化办公。
1、发文管理：支持发文审批、审核、复核、会签、签发的公文成文审批过程。
2、收文管理：支持收办件、收阅件处理，支持登记、拟办、会签、承办、办理、阅读、知会等节点动作。
3、签报管理：支持签报审批、审核、复核、会签、办理、归档等的签报处理过程。
4、公文审批：实现审核审批、签字、文单签批、提交意见等应用，为处理公文提供易用工具。
5、流程控制：支持公文流转过程中，通过公文模板支持公文流转的正式性、严肃性与规范性，实现公文管理的刚性控制；通过会签、多级会签、回退、终止等应用，支持公文流转过程中的异常情况处理。
6、查询统计：支持查看查询结果中的具体公文，包括公文流程、文单等，可设置多种查询

条件，符合各类查找要求，支持处于不同流转状态下的公文查询。
7、归档管理：支持电子公文归档和安全存放，确保公文归档保存的真实、完整、安全与可识别，提供公文文档库管理功能，实现公文分类、借阅，并记录相应操作过程。

1.5 知识管理

建立安全、分类、多级管理的知识文档管理体系，实现分中心知识文档库的构建。
1、文档目录：文档目录不限层级，且每个目录均可以进行权限控制。
2、文档权限：支持控制单篇文档的下载、打印、编辑、查看权限。
3、支持文档版本管理。
4、支持文档订阅功能。
5、文档搜索：支持全文检索，方便快速查询文档，通过模糊查询、关键字查询可在系统中快速查找需要的信息。
6、文档与流程关联：支持文档与流程关联，在创建文档同时可以自动触发相关流程进行审批。

1.6 会议管理

实现分中心会议会前、会中、会后的统一管理。
1、会议日历：支持以日历方式显示会议情况，可以按会议状态显示或者按人员组织来显示会议信息。
2、会议室管理：支持会议室的申请、审批、查询、使用统计、通知参会人等功能，避免会议时间和会议场地的冲突，实现会议统筹安排。
3、会议通知：会议流程发起后，可以设置通过即时通讯、邮件、短信平台等多种方式通知参会人员，并自动将会议自动安排进参会人员日程表。通知发出后系统自动发出回执给予参会确认，同时参会人员可自行下载权限范围内的会议相关资料。
4、会议决议：支持对会议纪要、会议决议的审批，形成历史会议记录，方便日后查询。
5、会议查询：支持多条件组合模糊查询会议状态。
6、会议与日程关联：支持会议预定成功后关联到“个人日程”功能，为参会人员创建会议日程。

1.7 车辆管理

实现分中心公务车辆的统一管理。
1、车辆信息维护：支持对车辆档案的基本资料维护、车辆保养维修记录等。
2、车辆申请审批：支持通过流程审批对车辆的使用申请。
3、车辆使用情况：支持以列表方式查看车辆使用情况，可以申请使用车辆，通过日期范围可以根据日、周、月来查看。
4、车辆查询：支持显示所有可查看的车辆，通过车牌、车辆类型、司机等信息搜索车辆。

1.8 日程管理

实现分中心员工日程的统一管理。
1、日程新建：支持对各级职工日程信息的新增、编辑、查看、检索等操作。
2、我的日程：支持查看个人工作日程安排，可以将日程进行共享。
3、所有日程：支持查看所有可查看日程，包括自己的日程和其他用户共享可以查看的日程。
4、日程查询：支持通过条件查询所有可查看的日程。

1.9 办公资产管理

1、支持实现行政办公资产生命周期管理，实现资产申请、入库、领用、借用、维修、报废等全过程生命周期的管理；
2、支持通过流程审批实现资产状态的变更，资产的分摊到人、到部门，并实现资产变更、库存，使用状态的统计报表。

1.10 移动办公平台

建立安全、高效的移动办公平台，实现随时随地的移动办公。

1、移动办公：提供移动办公平台，实现工作的移动处理，可支持IOS、安卓、鸿蒙等主流系统。

2、移动安全：支持通过移动终端的设备绑定方式来保障移动设备的安全性，并且支持多种安全验证方式来进行移动办公。

3、移动门户：支持移动门户建设，支持新闻、公告、待办、文件、留言、任务、会议等所有信息都能根据每一个人的岗位进行个性化推送。

4、移动审批：支持在移动终端上进行流程申请及审批、支持手写签名审批，并能够在移动终端上支持与流程相关的信息关联透视。

5、移动消息：支持通过移动端对个人待办事项进行提醒，支持在移动端实现员工实时互动、交流、沟通（包括点对点聊天、群聊等）。

6、移动文档查阅：支持在移动终端上查看本人有权限的文档信息。

7、移动会议：支持移动终端上查看个人会议安排、会议提醒等功能。

8、移动日程：支持移动端上查看个人日程安排、日程提醒等功能。

1.11 即时通讯

提供内部的即时通讯功能，类似微信功能，如单人、群组聊天，@他人、语音、拍照、文件、消息撤回、消息回执、聊天记录查询。即时通讯功能需要同时支持 PC 端和移动端，并且 PC 端和移动端可以实现消息同步、文件互传；PC 端和移动端可同时在线。

1.12 分级分权管理

建立内部分级分权管理体系，实现分中心与院本部应用与数据的独立。通过分级分权管理，实现统一管控，各下属单位通过分级管理员独立个性化维护自身单位门户、流程、文档等数据，既实现组织架构的相互独立，又实现前后端功能模块的相互独立。

1.13 系统安全要求

1、系统底层支持三员管理模式，即系统管理员、安全管理员、审计管理员三权分立，避免单个管理员权限过大；

2、服务器端存储的数据支持加密处理，保障数据存储安全；

3、用户密码加密存储，保证密码不会外泄。系统应能提供账户密码的更换周期控制、密码强弱度的校验等措施，有效保证用户密码的安全使用。

4、要求能实现 HTTPS 通道访问加密传输；

5、#能够充分考虑冗余、备份、容灾、故障快速恢复机制；

6、支持通过数据库安全隔离、系统数据的使用规范等措施提升数据安全；

7、支持在用户名和密码认证外，可以结合第三方认证，包括第三方统一身份认证等方式进行登录；

8、完善的应用级别权限控制：系统应能提供基于个人、单位、部门、群组、角色、岗位、级别的多维度权限控制，系统可以针对以上属性进行灵活的权限设定，确保信息安全的可定义性和可执行性。

1.14 其他要求

1、提供自验收通过之日起三年的质保服务。每年提供至少 4 次的免费上门维护保养工作。
2、★实现与医院现有协同办公系统的无缝衔接，分中心与医院之间办公流程可根据甲方要求无差别自定义设置。
3、#质保期内服务：根据分中心管理要求，为分中心指定的第三方的业务开发提供必要的技术支持，免费提供相应的数据接口和程序接口服务，不再额外收取接口费用。
4、中标方应对系统使用人员进行操作培训，直至使用人员熟练掌握为止，提供详细培训记录。

2. 阜外华中心血管病医院协同办公系统维保服务

1、服务方应指派专人提供服务，全权负责该项目相关的系统运作与技术支持。安排定期走访医院以及完成软件的升级安装、并保证医院能够在规定的服务及响应时间内得到相应的技术支持服务。
2、服务方负责承担系统的标准培训，指导、解答医院各业务部门有关系统的操作性问题。
3、负责处理系统中流程、文档目录、门户、组织权限调整及处理、解决数据调整、基础配置等维护类任务，负责业务流程调整和新增流程处理工作。
4、根据医院需求，提供运维支持服务，工作内容包含：问题处理、人员培训、系统 BUG 修复以及技术支持等。
5、服务方为系统故障的第一响应方，服务方有责任在医院要求的时间内首先响应医院的要求，并及时处理和排除故障。
6、#承诺服务响应时间为 7*24 小时，提供 7*24 小时的电话咨询、电话技术支持服务，如电话技术支持解决不了问题，承诺 2 小时内到达现场维护，4 小时内修复。特殊情况在 6 小时内无法修复的，维护期内服务方应予以使系统可正常运转的措施。
7、涉及到重大问题，影响系统正常运行的情况，在接到医院服务请求后 1 小时内到达现场解决，必要时安排高级别技术专家现场支持。
8、提供系统运行情况的定期巡检（每年不少于 4 次）及根据医院要求进行不定期巡检，并出具巡检报告。
9、#根据医院要求对系统进行修改，或为医院指定的第三方业务系统开发提供必要的技术支持与对接，免费提供相应的数据接口和程序接口服务，不再额外收取接口费用。
10、★提供符合医院要求的安全机制确保本系统的数据安全，保证数据不被非法利用和盗用。
11、定期对系统进行必要的安全补丁装载和系统安全升级工作，防止潜在故障的发生。

3.阜外华中心血管病医院协同办公系统版本升级

3.1 应用系统升级

★将医院现有系统升级至当前最新稳定版本，升级过程中不影响正常工作，确保现有数据及集成等内容安全迁移至新版本系统中。

3.2 移动端系统升级

★将医院现有系统升级至当前最新稳定版本,优化移动端后端存储机制，并增加鸿蒙等主流操作系统适配，确保移动端在鸿蒙等主流操作系统上正常使用。

3.3 系统功能优化

（一）系统性能优化

1、优化系统登录体验，提升系统登录界面加载速度。
2、优化系统门户界面，提升系统门户切换速度。
3、优化流程界面，提升流程新建、待办、已办查询速度。
4、#解决因 flash 插件停止更新导致的用户使用和后台维护的问题。
5、支持界面调整，系统字体大小调整，系统主题风格变化等。

（二）组织人事优化

1、优化组织人事功能，提升组织人事界面响应速度。
2、优化人事卡片界面，人事卡片上支持个人信息、工作信息的聚合展示。
3、优化通讯录功能，支持用户根据姓名、电话等方式快速找人，也可通过我的下属、同部门及按组织结构等多种方式，快速定位某个人。
4、优化新建人员操作，支持直接在新建人员界面维护登录帐号信息，也可到系统信息中重新分配帐号信息。
5、优化组织及人员维护操作，增加批量调整及批量编辑功能。

（三）门户管理功能优化

1、优化登录界面，新版本登录界面需支持“记住用户、记住密码”操作。
2、优化门户主题风格和界面布局，支持不同风格主题自由切换。
3、优化门户显示界面，增加字体调整功能，支持门户字体大小可随意调整。

（四）流程管理功能优化

1、新建流程界面优化，支持输入关键字，快速定位至所需流程；并优化新建流程界面排序方式。
2、优化流程表单界面，让表单必填字段更明显，有必填项未填时，提示更加明显。
3、优化流程图界面，支持将流程图中的操作者，直接显示为未查看、已查看、已办理。
4、优化流程处理意见框，支持关联附件、文档等操作。
5、优化流程打印功能，支持控制打印节点，支持设置打印次数。
6、优化流程抄送功能，接收到（抄送）的流程支持批量设置为已读。
7、优化待办事宜界面，在待办列表增加 “退回”和“代理”文字标识以及分别单独显示被退回、待阅、待处理待办事宜。
8、优化流程删除操作，支持流程回收站功能，支持恢复 30 天内删除的流程。

（五）知识管理功能优化

1、优化文档查询功能，支持收藏常用目录，支持在查询文档界面直接新建文档。
2、优化新建文档功能，使新建文档操作更方便。
3、优化文档批量共享功能，支持除了新增共享范围，也可同时修改原有共享。

4、增加知识中心功能，可在知识中心中集中展示我有权限看到的文档，我发起的文档，点评我的文档、我在系统中的知识贡献等。
5、优化知识删除操作，支持文档回收站，支持恢复 30 天内删除的文档。

（六）会议管理功能优化

1、优化会议日历功能，支持在会议日历界面直接新建会议、查看会议室使用情况。
2、优化新建会议功能，支持多会议室管理员设置，支持同时选择多会议室。
3、优化会议室管理功能，支持在会议室使用情况界面快速预览会议室情况。
4、优化会议管理功能，支持有权限用户可在前端直接新建会议类型、会议室等。

（七）日程管理功能优化

优化日程管理功能，直接显示“新建日程”按钮，支持直接关注部分人员日程，支持日程的批量导入。

（八）系统安全优化

1、优化密码及密保设置，增加二次密码功能，可设置在查看重要流程时必须输入密码二次验证，确保系统更安全。
2、#优化密码设置，新增密码找回方式设置，支持短信找回、密保问题、邮件找回等方式。
3、优化密码锁定功能，支持设置自动解锁。
4、优化隐私设置，支持对个人电话、手机号、电子邮件等进行隐私设置。
5、优化权限管理，支持底层三员管理模式，即系统管理员、安全管理员、审计管理员三权分立，避免单个管理员权限过大。
6、#优化应用漏洞补丁完善功能，提高系统整体的安全性。

4.用户数增加

1、★要求新增用户数可供分中心以及医院共同使用。
2、定期协助优化清理系统中用户数量，防止因长时间不登录、离职或其他原因占用有效用户数量。所优化清理的用户数量可作为新的用户授权使用。

包 3：智慧运维系统建设及数据库维保服务

一、机房动环监控系统建设要求

1.1 总体技术要求

总体技术要求中增加：

兼容对接原有控制平台（品牌：信锐； 设备型号：SIC-5030-IPSIP），提供与现有平台对接成功的证明截图，如若不能兼容则需要进行对现有设备的替换，并提供技术指标不低于现有总控平台的设备，以及将设备与施工费用体现在最终报价清单中，并提供相关证明材料并加盖公章，如未提供或不达要求则视为无效投标处理，下附现有总控平台技术指标

总控平台技术指标：

1、千兆以太网口数不少于 6 个；RJ-45Console 管理口不少于 1 个；USB 接口不少于 2 个;最大支持不少于 3000 个终端接入以及授权；

2、支持 modbus-assci ，modbus-rtu, shut，电总 QG，485、干接点、湿接点、SNMP 等多种协议，支持接口方式为 485、232、开关量

3、支持 3D 智能引擎，内置网络设备、机柜、UPS、办公资产等素材，可以基于机房真实情况，通过拖拽式真实还原，实现所画即所得

4、支持基于数字孪生技术的大屏展示，向管理人员展示整体机房整体运行状态，包括

UPS 状态、精密空调状态、电力系统、温湿度情况、告警情况等信息，数据通过友好的大屏直观呈现展示；

5、支持基于机房空间真实展现各个传感器和系统状态，并联动告警，同时在空间展示也出现颜色的变化，告警恢复后，颜色恢复成正常状态；

6、支持可视化呈现中心、智能告警中心、移动运营中心、全场景知识库等多个模块和功能，支持 3D 建模，可基于用户真实环境一比一还原；支持邮件、短信、电话、声光、APP、语音、微信、微信企业号、阿里钉钉、云守护等告警方式；

7、支持多分支机房统一管理，支持本地局域网部署和跨互联网远程部署，通过平台可以对所有分支的接入传感器和物联网关进行统一集中管理，包括统一策略配置、统一运行状态查看、统一数据分析；

★工期要求：项目合同签订后 7 天内完成项目的实施、联调、测试、部署等工作，并投入运行，进行项目验收。

1.2 具体招标要求

序号	产品名称	技术参数	数量	单位
1	配电柜监测	1、支持测量各相相电压有效值、三相相电压有效值的平均值、电压有效值、三相线电压有效值的平均值、相位角、1～4 回路各相电流有效值、有功功率、总有功功率，全回路总有功功率、各相无功功率、总无功功率、总视在功率、各相功率因数、总功率因数、各相有功电能、总有功电能，全回路总有功电能； 2、支持计量有功电能，掉电不丢失 ★ 3、支持采用 RS485 数字通讯接口采集所有数据，支持对接兼容现有平台，提供与现有平台对接成功的证明截图，加盖厂商公章，或者承诺可以与现有平台对接成功。（中标后如不能兼容，需要提供技术指标不低于现有总控平台的设备，并由中标人承担相关费用，直至满足采购人需求。） 4、电压支持：测量范围:30~600V(线电压)；20~400V(相电压)，PT:1~10000；连续过载：800V 5、电流支持：配互感器 withCT0~400A；直入型 0~6A；CT:1~10000；连续过载：2 倍 6、支持功率测量范围：单相功率：0~80000W/var 总功率：0~240000W/var/VA(按实际输入 3×U×I) 7、每套配备电流互感器等配件 3 个；	9	台
2	采集器	1、PRS485 接口≥1，DATA 接口≥1； 3、支持 MODBUS485、RS232 两种接口形式的数据采集及对接； 4、RS485 接口速率≥3Mbps，RS232 接口速率≥250kbps； ★ 5、支持通过软件自定义 RS485、RS232 接口线序，可实现 RX、TX、GND 的软件自定义，提供软件功能截图并加盖厂商公章 ★ 6、可以被数据采集设备统一管理，实现激活、上线、调试等操作；提供软件功能截图并加盖厂商公章 ★ 8、为确保物联网网络安全，设备制造商产品需符合《GB/T 37044-2018 信息安全技术物联网安全参考模型及通用要求》，须提供相关认证证书复印件、国家认证监督委员会查询截图和链接，并加盖厂商公章	65	台
3	蓄电池收敛模	1、支持蓄电池监测模块个数：≥240 节 2、支持组端电压检测：1~800V，	6	台

	块	3、电压精度，误差≤0、5% 4、组端电流：支持 1~3000A 量程的霍尔传感器，1%-0 精度（霍尔精度） 5、工作电源：DC12V 6、工作温度：-25℃～+85℃ 7、★支持与机房动力环境监测系统对接，实现告警、展示等功能联动，提供功能截图，并加盖厂商公章 ★ 8、兼容现有控制平台，提供与现有平台对接成功的证明截图，并加盖厂商公章，或者承诺可以与现有平台对接成功。（中标后如不能兼容，需要提供技术指标不低于现有总控平台的设备，并由中标人承担相关费用，直至满足采购人需求。）		
4	蓄电池监测模块	1、支持工作电压可选，范围 8.0V-18.0V； 2、工作功耗：< 0.05W； 3、电压检测精度：误差≤0.2%（8.0V-18.0V）； 4、支持电池温度检测，温度监测范围：-10～85℃； 5、温度检测精度：±1℃； 6、通讯接口≥2 个百兆网口； ★ 7、与蓄电池收敛模块、基础设施物理安全感知平台同一品牌，支持与蓄电池收敛模块搭配使用，按照电池数量配置；	480	台
5	电流霍尔传感器	1、电流量程：≥200A 2、与组端收敛模搭配使用； 3、监测组端电流、电压	6	台
6	蓄电池监测终端	1、支持 HDMI、VGA、485 等通讯协议，支持多种接口。 2、网络接口≥1 个百兆 RJ45 接口 3、支持 DC12V3A 供电 4、支持监测最高单体序号、最高电梯电压值、最低单体序号、最低单体电压值、最高温度序号、最高温度值、最低温度序号、最低温度值、单体总数、最低单体剩余容量。 5、这次监测环境温度、总续航时间、电压告警、电流告警、容量、可充电电量、可放电电量、组端 SOC、剩余容量、容量百分比、单体 SOC； ★ 6、支持与机房动力环境监测系统对接，实现告警、展示等功能联动，提供功能截图并加盖厂商公章	3	台
7	消防监测	1、支持本地供电 2、支持监控电流：＜4mA，支持火警电流：＜30mA 3、支持继电器干接点输出，监控时输出开路，报警时输出短路（用户可以自行设定） 4、支持指示灯提示，工作状态红灯常亮，检测有人员走动的时候红灯闪烁 5、支持自动报警且报警音量：＞80dB（正前方 3m 内） 6、支持正常工作温度：-10℃～+50℃，相对湿度：＜95% ★ 7、兼容现有控制平台，提供与现有平台对接成功的证明截图，并加盖厂商公章，或者承诺可以与现有平台对接成功。（中标后如不能兼容，需要提供技术指标不低于现有总控平台的设备，并由中标人承担相关费用，直至满足采购人需求。）	37	台
8	温湿度监测	1、支持温度、湿度数据采集与上报的机架式温湿度传感器； 2、支持采集温度范围：-10℃～70℃；误差<±0.3℃，在 25℃	78	台

		时测试； 3、支持采集湿度范围：5%～95%RH（无凝露）；误差<±3%RH，在 25℃时测试； 4、支持液晶显示：显示当前温度，湿度，网络连接状态； 5、支持 RS485 接口：通信协议：MODBUS-RTU 协议；波特率：默认 9600；可选 2400、4800、9600、19200bit/s；数据格式：N,8,1； 6、设备管理：支持平台统一集中管理，支持设备自定义命名 7、支持分组管理，要求不低于 6 级分组，包括地区、楼栋、楼层、部门、具体位置等； ★ 8、支持联动空调、加湿器、除湿器实现自动化控制；提供软件功能截图并加盖厂商公章 9、支持 Web 端、APP 端远程查看温湿度传感器数据，以及远程调节温湿度阈值； ★ 10、兼容对接原有控制平台，提供与现有平台对接成功的证明截图，并加盖厂商公章，或者承诺可以与现有平台对接成功。（中标后如不能兼容，需要提供技术指标不低于现有总控平台的设备，并由中标人承担相关费用，直至满足采购人需求。）		
9	漏水监测（不定位）	1、漏水反应时间≤2S 2、支持至少检测 200 米距离范围的漏水情况 3、支持兼容两芯或四芯测漏传感电缆 4、支持本地 12~24VDC 供电 6、存储温度-40° C 至 60° C，工作温度-20° C 至 50° C，湿度 5%到 95%（无冷凝） 7、要求搭配 15 米不定位漏水检测线缆，每套配置 1 根 ★ 8、兼容对接原有控制平台，提供与现有平台对接成功的证明截图，并加盖厂商公章，或者承诺可以与现有平台对接成功。（中标后如不能兼容，需要提供技术指标不低于现有总控平台的设备，并由中标人承担相关费用，直至满足采购人需求。）	64	台
10	空气质量监测(粉尘)	1、粒子粒径≤1μm 2、量程≥浓度：0~8.8 千粒/升 3、支持输出信号电流输出：三线 4mA~20mA 电压输出：0V~5V 或 0V~10V 网络输出：RS485 4、负载电阻：电流输出型：≤500Ω，电压输出型：输出阻抗 250Ω 5、系统精度≤±10% 6、平均功耗≤42mA	3	台
11	空气质量监测（氢气）	1、测量范围≥1000PPM 2、示值误差≤±1% 3、响应时间≤20 秒（T90）， 4、恢复时间≤30 秒 5、功率≤2.5W（DC24V） 6、支持三线制 4-20mA 电流信号输出，可连接各种报警控制器、PLC、DCS 等各种控制系统； 7、支持 RS-485 数字信号输出，连接 RS232 转接卡可在电脑上查看存储数据； 8、支持 2 组继电器高低段报警开关量输出（标配 1 组，选配 1 组）：无源触点，容量 30V1A、125VAC0.5A； 9、防护等级≥IP66	3	
12	红外入侵检测	1、工作电源：支 DC12V（可工作在 DC9-24V）。 2、探测距离≥12m	14	台

		3、探测角度≥90 度 4、探测速度≥0.3 米/秒~3 米/秒 5、防拆输出：常闭，接点容量 DC28V100mA 6、报警输出：常闭/常开可选，接点容量 DC28V100mA 8、支持 Web 端、APP 端远程设置设备状态 ★ 9、支持联动其他设备，如报警设备、视频监控设备等，提供软件功能截图并加盖厂商公章 10、支持在物联网平台可统一管理全部红外人体感应设备		
13	人脸识别门禁	1、支持触摸显示屏，可显示软件界面及操作提示，设备实时检测最大人脸，具有人脸框提示设计，方便用户校准； 2、支持采用宽动态摄像头，最大视场角 120°，面部识别距离＞2m，适应 1.2m-2.0m 身高范围，支持手机照片、视频防假，支持远程视频预览，支持识别二维码； 3、支持星光级图像传感器，无需白光补光灯，在暗光或无光环境下人脸识别效果不受影响； 4、设备采用深度学习算法，支持 5000 人脸库，人脸比对时间≤0.2s/人，人脸验证准确率≥99%，识别速度快，准确率高； 5、设备支持多种认证方式：刷卡、人脸、刷卡+人脸等认证方式 6、设备支持普通卡/残疾人卡/黑名单/巡更卡/来宾卡/胁迫卡/超级卡/解除卡等多种卡片类型。 7、设备支持多重卡开门功能、首卡开门功能、超级卡和超级密码开门、中心远程开门、多重卡认证+远程授权（N+1）开门功能、在线升级功能、单门反潜回功能； ★ 8、设备支持统一管理。提供对接成功截图，并加盖厂商公章 9、含磁力锁、开门按钮、电源等配件包，每台含 1 套配件包	5	台
14	数据采集设备	1、以太网口数≥3 个；Console 管理口≥1 个；USB 接口≥1;PDI 接口≥4 个，PRS485 接口≥5 个，DO 接口≥1 个； 2、支持门禁主机功能，具备专门的门禁接口，电源接口≥1;干接点开关接口≥1 个；韦根接口≥1 个； 3、内存≥8GB； 4、所有接口均支持 RJ45 形态，支持对外提供 24V 直流供电； 5、支持传感器类型智能识别，智能上线； 6、支持在多分支机房场景下，与总部网络中断时，本地机房关键数据可以在采集主机实现缓存，时间周期大于 15 天，网络恢复时，数据自动补传给总部平台，保障数据不因网络中断而丢失。 7、支持直接接入声光告警模块和 4G 电话告警模块，在多分支机房场景下，与总部网络中断时，如果分支机房出现风险时，采集主机可以直接实现声光告警和电话短信告警。 ★ 8、兼容对接原有控制平台，提供与现有平台对接成功的证明截图，并加盖厂商公章。（或者承诺中标后如不能兼容，则需要对现有设备进行替换，并提供技术指标不低于现有总控平台的设备，直至满足采购人需求。） ★ 9、为保证设备扩展性，要求设备制造商软件开发能力达到 CMMI 五级，提供相应证书复印件并要求设备制造商盖章证明	32	台
15	声光报警器	1、报警音量：MAX110dB； 2、工作电压：交流 9V～18V 或直流 12V～24V； 3、工作环境：-35℃～55℃； 4、控制方式：采用 Modbus 协议，通过网口形态 RS485 接口与	3	台

		物联平台进行通信； ★ 5、联动告警：支持联动机房动力环境监测系统实现多样化报警，如设备异常、非法入侵、机房漏水、温度过高等告警，支持同时发出声、光二种警报信号；提供支持功能截图并加盖厂商公章 6、支持被机房动力环境监测系统管理、配置、展示；		
16	视频监控对接系统	1、能够与现有视频监控系统进行对接，支持对接 ONVIF 协议摄像头 2、对接后可直接调取监控画面，查看告警事件	1	套
17	设备接入软件	机房关键设备接入数量≥46 基础设备接入数量≥295	1	项
18	功能对接软件	支持 UPS 接入 支持精密空调接入	1	项
19	售后服务	提供 3 年特征库升级服务，提供 3 年 7*24 小时原厂售后服务，要求设备厂商在有售后服务团队，针对本项目提供原厂售后服务承诺函，加盖原厂公章。	1	项
20	辅材	包含但不限于网线，水晶头，信号线等其他施工过程中需要使用的材料	1	套
21	施工安装服务	包含本次项目中各个设备的安装、网络布线以及其他施工工作	1	项

二、信息化智慧运维管理系统采购需求建设要求

1. 需求说明

现有信息化运维工作中的资产、工作流等管理往往依赖于人工记录和静态表格，难以实时反映资产的动态变化，且存在安全隐患等问题。同时，现有工作流程涉及多个环节、效率较为低下，这不仅在一定程度上增加运维成本，也会影响信息中心运维业务的连续性和服务质量。

为进一步加强信息化运维工作的效率、安全性，本项目旨在通过信息化手段，实现信息中心各类资产的动态管理和重大问题的实时监控，确保运维人员能够随时掌握资产的最新状态，及时发现并解决潜在问题。同时，本项目融合工作流管理板块，能够随时随地处理运维过程中的各种工作流程，如新设备上线、故障处置、配置变更等，实现对运维环境的全面监控和优化，提高运维效率、准确性和智能化水平，从而为信息化运维工作的持续发展和运维业务创新提供有力保障。

2. 技术要求

2.1. 操作维护

从目前用户的使用技能、接受程度以及系统的维护成本考虑，软件系统应该具备以下特点：采用 B/S 架构；安装部署快速、简单；无需安装用户端，通过网络浏览器使用系统功能；系统更新、维护只对服务器操作，用户端无感知。

2.2. 安全性

对于系统的安全方面，要能保证关键数据的安全性，要能做到信息加密，要能对身份进行辨识，对权限进行严格的控制，要能保证传输过程的安全性，要能对系统的操作做好系统日志。系统部署在内网环境中。

2.3. 可靠性和稳定性

系统应采用微服务架构，确保系统能够实现长期稳定运行，避免宕机事件的发生。系统建设分为两个阶段：

上线初期：在这个阶段，应建立一个核心用户微信服务群，以满足用户的基本需求。高度重视用户的反馈，对于用户提出的建议和优化需求，需要迅速响应，并及时更新系统以提

升用户体验。

后期稳定期：当系统进入稳定运行阶段，将通过客服热线和微信群提供全天候（7*24小时）的客户服务支持。对于严重异常BUG，需要组织团队在一小时内进行处理，并尽快恢复系统的正常使用，以最小化对用户的影响。

在数据安全方面，需要采用了先进的数据库技术，包括双机热备，以确保数据的冗余性和安全性。这些措施将有效防止数据丢失，保障用户数据的完整性和可靠性。

2.4. 拓展性

在系统建设中要满足信息资产管理和运维流程的功能需求外，还要考虑系统能够随着组织结构、业务流程和技术工具的变化而进行相应的调整和升级，能够与其他现有的软件系统的兼容性，对重要资产做监控与告警，通过多种渠道发送告警通知，并在告警未处理时提升告警级别，使得运维各负责人能够及时发现并处置资产异常状态，提升运维效率。

3. 建设要求

3.1. 服务端开发要求

3.1.1. 项目说明

该采购需求包含系统设计、前端程序、服务端程序和数据库设计开发部分。

3.1.2. 语言要求

服务端采用Java、Go、node、php、python等主流开发语言，数据库采用MySQL数据库。

3.1.3. 联调测试

前后端根据项目实际需求，提前约定数据结构和API规范，代码开发完成后启动接口联调测试工作，其包含接口调用数据安全、存储安全、权限校验、单元测试、联调测试和安全部署策略等。

3.1.4. 服务部署

项目代码部署在内网的生产环境和测试环境两个版本。对于需要上线的内容，需要在测试环境运行通过验收后，方可发布到生产环境。如遇到紧急问题，需支持代码紧急回滚，做好紧急预案。

3.1.5. 服务运维

自项目验收通过取得项目验收报告之日起，提供3年的免费维保服务。

3.2. 前端开发要求

3.2.1. 前端框架

采用主流的前端框架，如 React、Vue 或 Angular，便于可读及维护，以提高开发效率和代码可维护性。

3.2.2. HTML/CSS

使用HTML5和CSS3规范，构建符合标准、响应式的页面布局，确保在各种设备和浏览器上的兼容性。

3.2.3. JavaScript

使用 JavaScript 作为主要的客户端脚本语言，实现页面交互、动态渲染等功能。

3.2.4. 组件化开发

通过组件化开发模式，将页面拆分为多个可复用的组件，提高代码的模块化和可维护性。

3.2.5. RESTful API

采用 RESTful API 设计风格，与后端进行数据交互，确保数据传输的高效和稳定。

3.2.6. 页面性能优化

对前端页面进行性能优化，如图片优化、懒加载、代码压缩等，同时支持缓存请求，以提高用户体验。

3.3. UI设计要求

3.3.1. 界面设计

设计具有现代、直观和用户友好界面的管理系统，确保符合客户的品牌风格和要求；提供多个设计方案供客户选择，并根据反馈进行修改。

3.3.2. 用户体验优化

分析用户需求和使用情况，设计流畅的用户体验路径，确保系统易于操作和理解；使用最佳实践和用户界面设计准则优化界面，以提高用户满意度和系统使用效率。

3.3.3. 响应式设计与兼容性

确保管理系统在各种设备和屏幕尺寸上具有响应式设计，并且兼容性良好，主要是 PC 浏览器。在多个浏览器上进行测试，确保与流行的浏览器如 Chrome、Firefox、Safari 和 Edge 兼容。

3.3.4. 布局与导航

采用清晰的布局，便于用户快速找到所需数据和功能；设计直观的导航结构，减少用户寻找信息的步骤；使用面包屑导航、侧边栏或顶部导航栏，以增强导航的直观性。

3.3.5. 视觉设计

保持界面整洁，避免过多杂乱的元素；使用颜色、图标和字体来强调重要元素，同时保持视觉一致性；设计响应式界面，确保在不同设备和屏幕尺寸上都能良好显示。

3.3.6. 交互设计

确保交互元素（如按钮、链接）易于点击，且反馈明确；对于数据上传、下载、编辑等操作，提供明确的指示和进度反馈；设计合理的数据展示方式，如表格、图表，以便用户快速理解信息。

3.4. 平台功能

3.4.1. 组织架构和人员管理

本系统遵循现有的组织机构管理模式，设置组织架构、职务权限、账户管理，关联组织、职务、人员三者的统一，在每一层级的机构中有不同的职务和权限，实现责权分明。

3.4.1.1.组织架构管理

支持创建和管理多层次的组织架构，允许自定义组织架构的层级和结构，并支持配置对应组织的主管人员信息。

3.4.1.2.职务管理

支持定义不同的职务，每个职务分配不同的系统操作权限和数据权限。确保员工只能访问其权限范围内的功能和数据。清晰展示职务对应的成员列表。

职务需要具备：系统管理员、运维负责人、网络负责人、审计员等权限，每个职务有对应的权限。

1） 系统管理员：具有系统最高管理权限，通过管理员账户可以进行系统管理、资产管理、运维工作流管理、项目管理、策略模板管理、监控告警管理、台账管理、数据统计分析等。

2） 运维负责人：通过系统管理员分配给运维负责人对应管理权限。可以完成对负责的资产管理、相关运维工作流程的提交和审批、负责项目的管理、负责资产的告警管理及相关统计数据。

3） 网络负责人：通过系统管理员分配给网络负责人对应管理权限，核心定位在网络设备资产。可以完成对负责的资产管理、相关运维工作流程的提交和审批、负责项目的管理、负责资产的告警管理及相关统计数据。

4） 审计员：负责监督和审查系统的操作，确保所有操作符合安全规范。审计员的权限主要分为：查看操作日志、查看系统登录日志、运维流程审批等，确保系统操作的合规性和安全性。

3.4.1.3.人员管理

支持系统人员管理，系统管理员可创建、修改、启用、禁用和删除系统账户，包括用户名、密码、权限等的设置。

3.4.1.4.系统登录

支持用户名、密码、动态令牌登录。系统登录密码支持密码强度校验和完善的登录验证机制，防止暴力破解。

3.4.2. 系统首页

★ 系统首页应支持：运维流程快捷入口、资产动态展示、资产分类统计、待办事项、消息通知等信息，提升系统便捷性和易用性。

3.4.3. 资产管理

3.4.3.1.机房机柜可视化

★ 实现机房内部机柜及其内部设备的直观展示，支持清晰地看到每个机柜的布局、设备摆放情况；支持实时更新机柜及其内部设备的状态信息，如是否在线、网络波动等。

支持机房管理，可以便捷添加机房信息、管理机房状态、机房机柜配置等。

支持机柜可视化展示和管理，能够配置机柜规格、机柜位置等信息。系统中机房机柜可视化展示效果符合采购人机房、机柜的实际情况。

支持资产数据自动关联至机柜：通过完善的运维流程，将运维流程中收集的资产信息自动关联至机柜对应位置，实现机房－机柜－资产的可视化展示效果。机柜可视化展示效果中应展示资产的位置、资产状态等概要信息，提升资产运维效率。

3.4.3.2.资产库

★ 实现记录每一台设备的详细信息，包括设备类型、型号、序列号、购买日期、维保信息等，并实时更新设备的状态信息，如是否在线、是否故障等，支持通过系统查询和追踪资产的全生命周期信息，实现对资产的精细化管理。

资产库信息维护方式支持资产批量导入、从运维工作流程中获取等。

1） 资产批量导入：依据给定的 Excel 或 CSV 格式的模板，批量导入 Excel 或 CVS 中的资产数据至资产库中。

2） 从运维流程中自动获取资产信息，并将资产信息纳入资产库中，实现基于“运维工作流”的资产管理体系。

3.4.3.3.IP 管理

满足对 IP 地址的高效管理，跟踪每个 IP 地址段的使用情况，避免地址冲突和资源浪费。针对此目标需要具备 IP 地址管理功能、IP 地址分配功能。

IP 地址管理：支持 IP 地址段的列表展示、IP 地址段添加、IP 地址使用情况展示。展示内容包括：网络范围、子网掩码、描述、使用率等内容。

IP 地址分配：支持展示 IP 地址分配的资产信息，提供自动收集运维流程中对资产分配 IP 的功能，并统计当前 IP 段的使用率。

3.4.3.4.资产重要属性加密存储

对资产密码等重要资产信息进行加密，系统中对重要资产信息加*展示，不直接展示明文信息，查看资产重要属性需二次认证通过后方可展示。

3.4.4. 运维工作流

3.4.4.1.支持符合运维工作的流程

系统应支持新设备上线、故障处置、设备变更、安全策略变更、设备维修等类型的运维工作流程，覆盖信息化资产的上线、部署、维护、变更、监控、下线等全生命周期，并将全生命周期的资产信息自动归纳到资产库中，实现基于“运维工作流”的资产管理体系。

功能包括：支持查看待我处理的流程、已处理的流程、我提交的流程、抄送我的流程。

支持流程关键词、流程状态、流程类型等内容搜索。

3.4.4.2.实现自动化任务分配能力

系统应支持自动将工作流分配给相应的人员或团队，相关责任人完善资产信息，实现责权分明。

3.4.4.3.实现实时监控与提醒

系统应支持实时监控工作流执行情况，并在关键节点发送提醒。

3.4.4.4.实现流程可视化能力

系统用户可以查看自己所负责工作流的处理进度并处理涉及自己的流程，实现流程可视化。

3.4.4.5.历史记录与数据分析能力

支持记录并存储工作流的详细信息，并支持历史数据分析。系统应支持查看工作流的处理进度。

3.4.5. 策略模板

- **实现策略模板管理**

支持展示出口防火墙、网闸等设备的策略模板。模板内容涵盖但不限于访问控制规则、流量过滤规则、应用层过滤策略、安全域等，为资产设备的策略配置提供参考基准。

3.4.6. 项目管理

3.4.6.1.项目管理

支持项目信息的查询：包含项目名称、项目燃尽图、项目里程碑、台账情况等信息的展示，同时提供项目状态、项目名称、项目时间等内容的搜索。

项目管理首页支持项目总体情况的统计，包含：项目总数、进行中数量、已延期数量、已完成数量、已取消数量等项目数据。

3.4.6.2.项目时间管理

支持项目负责人设定项目的预期启动日期、预期完成日期，记录项目的实际结束日期；

3.4.6.3.项目里程碑管理

支持设定项目中的关键里程碑，如重要阶段完成等；支持监控里程碑的完成情况。

3.4.6.4.项目成员管理

提供项目成员列表展示，支持管理员添加项目成员。加入项目的成员才有权限查看项目进度、项目时间、项目里程碑、项目文档等信息。

3.4.6.5.项目进度监控

支持监控系统各里程碑的完成情况，支持通过百分比+进度条的形式展示项目进度；当项目进度滞后于计划时，支持发送消息提醒。

3.4.6.6.项目问题管理

支持项目成员记录项目在执行过程中遇到的问题，包括问题描述、影响范围、解决状态等，并跟踪解决状态。

3.4.6.7.项目文档管理

支持项目文档的管理，包括上传、下载和管理等，便于项目成员协作与共享。

3.4.7. 告警

3.4.7.1.资产状态监控能力

★ 支持实时监控各类资产设备的状态，包括但不限于服务器、网络设备、网络安全设备等；支持实时触发告警，支持持续监控丢包率等关键指标，及时发现网络波动或异常情况。

3.4.7.2.告警通知能力

支持通过短信、钉钉、企业微信等渠道将告警信息通知到相关运维人员，提升告警的及时性；当告警长时间未处理或问题升级时，支持提升告警级别。

运维人员收到资产告警通知后，需要及时处置告警信息，处置完成后需要在系统中标记处置结果。

3.4.7.3.告警历史

系统应记录所有告警的历史信息，包括告警时间、类型、处理状态等。支持告警信息的查询检索。

3.4.8. 台账

3.4.8.1.工作台账

工作台账主要用来记录日常工作。系统应支持工作台账管理、台账查询与检索、台账添加等功能。

工作台账展示数据支持：台账类型、工作类型、涉及资产、台账内容、台账状态等台账信息展示。并包含提交给我的、我提交的工作台账数据。

台账功能支持信息中心人员记录日常工作情况，包含：故障处理、安全事件处置、策略变更、巡检以及具体的工作内容。

3.4.8.2.项目台账

项目台账主要记录项目进度和项目问题，将运维日常工作和项目管理紧密结合。

支持项目台账管理：包含提交给我的、我提交的项目台账数据。项目台账展示数据支持：台账类型、所属项目、台账内容、台账状态等信息展示。

3.4.9. 系统权限控制

3.4.9.1.用户职务管理

系统应支持定义和管理用户职务，包括但不限于管理员、运维人员、审计等；应支持职务的创建、修改、删除和权限分配。

3.4.9.2.权限分级管理

系统应支持定义不同级别的权限，以适应不同职务的需求；应支持权限的细粒度管理，如查询、修改、删除、禁用等。

3.4.9.3.数据权限控制

支持基于职务的数据权限控制，可以设置个人、所属部门、所属部门及下属部门、组织的数据权限控制。

3.4.9.4.支持字典管理

具备字典管理功能，便于分类存储不同的数据项。

3.4.9.5.日志记录

支持系统使用记录、登录日志的记录，满足系统审计要求。

4. 性能指标参数

4.1. 系统安全设计

- 程序开发：消除各类 SQL 注入、DDOS 攻击、跨站脚本等主要应用安全漏洞；
- 网络安全：按照国家相关标准法规划定信息安全域和信任域，加强系统信息安全管理；
- 数据安全：数据库核心数据采用加密设计，且不存放用户明文密码。
- 非内网数据和内网数据交互时，需要部署前置机，通过网闸进行有限数据交互。

4.2. 系统性能设计

后台系统访问的并发访问用户不少于 100 个，业务操作响应平均在 1 秒以内，单用户的信息发布时间要在 3 秒以内。

5. 售后服务及其他要求

5.1. 项目实施要求

5.1.1. 工期要求

★项目合同签订后 15 内完成项目的功能开发、联调、测试、部署等工作，并投入运行。

5.1.2. 项目交付内容

成交人必须提供系统设计、部署、使用教程等相关电子文档和纸质文档，提供系统源代码、系统数据库及系统部署所需的相关软件。验收时成交人必须提供系统需求说明书、系统使用说明书、操作手册等有关技术文档。

5.2. 培训要求

对系统平台使用进行全面培训，提供针对本系统的管理人员和使用人员的培训方案。

使用人员培训≥4 次，管理人员培训≥3 次，制定相关图文版说明书。

5.3. 保密要求

任何一方对合作过程中获得的其他两方的商业秘密及其他与利益相关的数据或者信息负有保密义务，未经其他两方书面同意，不得向任何第三人披露或泄漏。三方的保密义务不因本协议的解除或终止而免除。

5.4. 服务要求

- 服务运维：自项目验收通过取得项目验收报告之日起，提供 3 年的免费维保服务。
- 应急修复时间要求：30 分钟恢复系统正常运行。
- 全年故障时间小于 12 小时，平均故修复时间小于 3 小时。

5.5. 部署要求

系统部署至内网私有云，由采购方提供部署所需的私有云服务器及数据备份服务器。

三、数据库系统维保服务要求

1、维护的范围和期限

（1）为招标人的信息系统数据库提供维保服务，包含但不限于现有信息系统数据库的技术运维服务，新增系统数据库的运维服务，数据库知识培训服务，数据库迁移、升级、优化及技术交流等服务；

（2）维护期限：自合同签订之日起 1 年。

2、维护工作内容和标准

总体描述：客户服务项目经理与支持团队；数据库问题、巡检与分析服务；数据库问题快速响应与定位服务；工程师快速现场支持服务；数据库迁移、数据库升级与优化服务；数据库知识培训服务；数据恢复验证及紧急恢复服务；现场值守服务、数据库运维安全服务和其他服务等内容，能够有效帮助招标人技术支持人员维护信息系统数据库的稳定运行，满足招标人对数据库高效、稳定运行环境的需求。

（1）客户服务项目经理与支持团队：

服务团队能力达到运维能力成熟度 ITSS 二级及以上。

在数据库维保期内，中标人需建立本地服务团队，需指定专职项目经理、专责服务人员、专责工程师团队等；

投标人中标后，指定一名项目经理，制定服务计划，联系服务资源，定期与招标人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从招标人相关人员的安排。 项目经理的更换须得到招标人同意。

投标方应对本项目提供满足项目实际需求的技术服务团队，其中一线工程师（驻场）1 名，二线高级工程师（非驻场）应配备相应类别人员，应当具有数据库以及其它相关技术栈的人员。具体人员要求如下：

★1、一线工程师（驻场，1 名）：一线驻场工程师须具有 5 年以上工作经验，在招标人指定地点开展工作，负责数据库的现场维护服务和其他相关工作。能够熟练操作 Windows server、Linux 等操作系统，熟悉常见备份软件和设备；能够根据运维工作需要，针对监控、例行维护、日常变更等场景自行编写脚本，实现自动化监控运维。

驻场工程师须具备 Oracle 数据库大师（OCM）水平相当的能力并熟悉达梦、人大金仓等国产数据库（需提供工作简历、能力证明材料等，工作简历应当包含工作时间、承担工作内容、证明人联系方式等内容）。

★2、二线高级工程师（非驻场）：二线团队应具有数据库，操作系统等相关技术栈的服务能力和丰富的工作经验，二线团队中应配备 Oracle 数据库工程师，国产化数据库类、操作系统类工程师，负责支撑一线工程师开展现场维护工作以及各类重大故障的现场支持。其中 Oracle 数据库工程师须具备 Oracle 数据库大师（OCM）认证的能力；国产化数据库类工程师应具备独立运维主流国产化数据库（如：达梦、金仓、OceanBase 等）的能力；操作系统类工程师应具备独立运维支持裸设备操作系统的能力。（需提供工作简历、能力证明材料等，工作简历应当包含工作时间、承担工作内容、证明人联系方式等内容）

3、服务期内，投标人不得擅自调换驻场工程师，如确需更换驻场工程师，需经投标人同意并提供符合要求的服务人员；若驻场工程师无法满足招标人的工作要求，招标人有权要求更换驻场工程师且不另外支付费用。投标人更换驻场工程师的时间为交接期，交接期从招标人同意更换驻场工程师或招标人提出更换驻场工程师开始计算，到更换的驻场工程师能够满足招标人要求为止，此交接期不计入驻场服务期内。

★ 4、投标方提供的以上各岗位工程师，需提供劳动合同、近 6 个月社保缴纳证明材料等，还应提供相关证明材料，证明技术服务人员具备项目所需的各项技术能力。

（2）数据库问题处理、巡检与分析服务

招标方应提供及时处理数据库运行过程中出现的各种问题的服务;定期对在用信息系统数据库进行巡检服务（至少每个月一次），对系统数据库的运行状态进行检查和分析，并提交正式的巡检服务报告；定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便招标人了解维护状况，及时预见并解决潜在问题。

（3）数据库问题快速响应与定位：

投标人提供服务期内每周 7 个自然日(含节假日)，每个自然日 24 小时的 7×24 全天候随时响应服务。投标人必须提供 7×24 小时固定热线电话号码、响应工作流程。响应时间指招标人发现问题，电话通知投标人时开始计算，投标人必须在 15 分钟内完成以下内容的初步判定：故障级别、影响范围、解决所需资源、解决时长。并按照故障的不同级别，遵循后文描述的不同级别所对应的服务时间要求。

（4）工程师快速现场支持服务：

当招标人根据系统、硬件出现故障或其他重要情况，要求投标人提供二线工程师现场支持服务时，从投标人接到招标人通知（电话、 短信、微信等）时开始，投标人二线工程师必须在 2 小时内到达招标人指定的现场，并立即开始现场不间断工作支持服务，根据诊断结果提供进一步的处理方案。当出现的问题不能判断属于硬件或系统软件层面时，维保工程师须和其它厂家工程师一起会诊，讨论出可行的测试方案，定位故障。

首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以招标人定义为准），均视为通知已到达并开始计算时限，如不能按时（2 小时内）抵达现场，每次处以 2000 元人民币罚款。一年服务期内，累计超过 3 次不能按时抵达现场的情况，招标人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

故障级别定义及服务级别要求

1.故障级别定义：

一级故障(重大故障)：最紧急，指系统软件在运行中出现宕机或系统瘫痪等导致服务中断、业务停止、数据丢失的故障。

二级故障(严重/主要故障)：紧急，指系统软件在运行中出现的直接影响服务，导致系统性能或服务能力部分丧失的故障(如系统软件部分节点故障,整个系统响应速度大幅下降)；或具有潜在的系统瘫痪或服务中断的危险，可能导致系统软件的基本功能不能实现的故障（如冗余系统单侧故障）等。

三级故障(一般/次要故障)：一般，除一、二级故障外的其它故障，指系统软件在运行中出现的，轻微影响系统功能和性能（性能降低小于 20%），但关键业务不受影响的故障。

2.故障处理基本要求：

故障处理时，优先考虑系统恢复以保证业务正常运行，然后再彻底解决故障。

3.故障响应和解决时限要求：

一级故障：15 分钟内响应，2 小时内到达现场，半小时内恢复系统，4 小时之内解决故障。

二级故障：15 分钟内响应，2 小时内到达现场，1 小时内恢复系统，12 小时之内解决故障。

三级故障：15 分钟内响应，2 小时内到达现场，4 小时内恢复系统，24 小时之内解决故障。

（5）数据库迁移、升级与优化服务

在招标人信息系统进行切换、升级、改造及硬件更换等重大事件时，投标人应派二线高级工程师提供数据库迁移服务；当数据库发现漏洞或厂商发布新的补丁时，投标方应提供漏洞修复或补丁升级服务；投标方应根据信息系统数据库运行情况，定期或不定期向招标方反馈数据库优化建议并提供相应服务。

（6）数据库知识培训服务

数据库系统软件的稳定、性能、安全等情况与信息系统的稳定运行密切相关，投标方应定期（至少每季度一次）根据运维工作情况为招标人举办免费的数据库知识培训。培训对象为招标人各应用系统管理人员、数据库管理人员等；培训内容主要包括数据库日常管理、常见及紧急故障处理办法、相关新技术的介绍等；培训要针对实际维护工作，同时兼顾理论；培训形式可采用现场或实操讲解等。

（7）数据恢复验证及紧急恢复服务

投标人根据招标人需求，定期（至少每季度一次）对信息系统开展备份数据恢复验证工作，并出具数据恢复验证报告。

服务期内，若生产环境数据出现异常，需要使用备份数据进行恢复时，投标方应当提供相关技术服务及支持人员，持续不间断进行数据恢复，确保生产系统恢复运行。

（8）现场值守服务：

在招标人信息系统发生故障、重大事件、关键时点、系统升级、运维保障等情况下，投标人应派二线高级工程师到达招标人现场，提供现场值守服务。

★（9）数据库运维安全服务

中标人应在招标人现有网络环境部署数据库运维相关工具，对运维人员的数据库运维提供安全保障服务。该运维工具应当支持对招标人不少于 60 套数据库（每套数据库为双节点 5 个 IP 或单节点部署）提供运维安全保障。

运维工具应当包括数据库准入，访问控制，数据库字段过滤及脱敏，运维审计，授权审批等多种功能。在访问控制和数据库准入方面，能够实现数据库真实账号和该系统账号映射绑定，使运维人员无需知晓数据库真实用户名密码即可开展工作，支持通过客户端访问系统提供的代理地址连接数据库；在数据库字段过滤及脱敏方面，能够实现数据库表级和行列级

的控制过滤，并针对不同运维权限账号，可查看到不同内容，针对查询到的敏感数据，可实现实时动态脱敏，确保在运维中的数据防泄漏。在运维审计方面，能够实现 SQL 命令的细粒度审计和分析，并详细记录用户行为。在授权审批方面，支持运维人员在授权审批后，执行相关高权限操作。

服务期内，招标人可免费使用该运维工具提供的数据运维安全服务，且相关系统资源可升级；服务期满后，相关运维工具资源应可继续免费使用,并免费提供该运维工具的安全漏洞补丁。

（10）其他服务

投标方在数据库问题处置完毕后，需向招标方提供数据库问题原因分析报告；

3、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。招标人不统一组织投标人对运维现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

包 4：机房及弱电维保服务

一、机房基础环境维保服务要求

1、维护工作范围

★（1）投标人为采购人列间空调、精密空调提供 1 年产品可溯源原厂维保服务，服务标准为 7x24 小时级别，参保设备维护期限为 1 年，自合同签订之日起。

★（2）维保服务包含：提供 20 台列间空调、9 台精密空调的原厂维保服务，提供 9 套 UPS 系统的巡检及电池放电测试服务，提供 3 套模块化机房内部动环监控主机 RDU-A 北向协议开发服务（提供厂商承诺函）。

（3）具体清单如下：

系统	设备名称	品牌	型号	数量
空调系统	列间空调	华为	NetCol5000-A	20 台
	精密空调	维谛	DME12	9 台
	空调滤网、耗材	国产		1 项
	室外机冲洗	国产		1 项
UPS 系统	UPS	华为	UPS5000-E	4 套
	UPS	维谛	400KVA	2 套
	UPS	易斯特	20KVA/40KVA/80KVA	3 套

模块化机房内部动环监控主机	RDU-A 北向协议开发	维谛	RDU-A	3 套

2、服务期限

维护期限：自合同签订之日起 1 年。

3、服务方式和内容

3.1 服务方式：

1）电话远程服务

乙方技术人员提供 7*24 小时电话支持和远程方式支持，接到甲方 UPS 或精密空调报修电话后，立即安排相关技术人员与甲方对接，进行远程电话指导或远程处理故障，使设备快速恢复正常。

2）紧急排故

运维期内，在 UPS 和精密空调运行过程中监控机房所报故障，包括故障定位、原因分析、故障排除及协调厂商服务等，乙方技术人员 5 分钟内响应，1 小时内到达现场并在 24 小时内解决故障。

3）日常巡检和维护保养

为确保维保 UPS 和精密空调正常稳定运行，做到有问题提前发现，每季度对精密空调进行现场巡检和维护保养，保证机房精密空调安全平稳高效运行，通过巡检可对 UPS 和精密空调设备存在的潜在安全或故障隐患进行分析并提出相应的解决方案后加以排除。

巡检周期：每季度进行一次现场巡检。

4）其它服务

按照甲方要求任何时间段重要活动的计划外和计划内到场服务。技术人员 1 小时内到达现场，进行现场技术支持服务。

3.2 服务内容：

1）硬件保修服务

★对列间空调和精密空调维保设备清单中的硬件提供可溯源原厂保修服务：一旦设备出现故障，维保方需提供必要的维修服务和解决方案，提供原厂替换件并负责更换，对符合条件的事件进行补救。在得到用户确认后维保工程师才能离开现场。

2）系统或硬件故障排除

UPS 和精密空调系统或硬件出现故障时，维保工程师到达现场，若非介质故障，应及时排除。

3）备件时效

备件返修/备件先行服务时效为工作日 8:30-12:00,13:30-18:00，以 15:30 为界，15:30 之前收到的申请当天进行处理，15:30 之后收到的申请第二个工作日进行处理。

4）响应时限

技术人员 7*24 小时电话支持和远程方式支持，获得与硬件问题相关的技术咨询或故障排除帮助。对于非硬件故障，1 小时内积极协助解决问题。对于硬件故障，2 小时内到达现场，若非介质故障，24 小时内完成维修服务。

5）巡检服务及电池放电测试

★每季度进行一次现场巡检，对 UPS 和精密空调维保清单设备进行现场硬件设备和线路巡检，包括各个配件的检测、链接状态、整机运行状态检测，每季度提供巡检报告。每年进行不少于 2 次的电池放电测试、UPS 切换测试，检测 UPS 运行状态。

6）RDU-A 北向协议开发服务

★提供甲方现有维谛模块化机房内部动环监控主机 RDU-A 北向协议开发，用于第三方动环系统的对接，实现现有动环监控相关模块数据的对接联动。

4、项目实施要求

4.1 机房基础环境设备维保服务要求

维保公司负责对数据中心机房基础设施开展维护保养工作，并记录维护保养结果。具体维护保养要求如下:

1）列间及精密空调维护保养工作内容

序号	项目	内容	频率
1	操作面板主板	检查显示是否正常、有无报警信息	1 次/季度
2	风机	听有无异常噪音，电流是否正常。	1 次/季度
3	加湿器	检查加湿器功能是否正常，视情况进行更换或清洗	1 次/季度
4	蒸发器	检查蒸发器下方积水盘排水是否畅通	1 次/季度
5	冷凝器	检查冷凝器是否按照系统内压力进行调节风机转速	1 次/季度
6	压缩机	检测压缩机工作电流是否正常、听有无异常噪音、检查有无液体渗漏	1 次/季度
7	电气检查	检查电源参数是否正常、检查新路器闭合状态是否正常，检查各进出线压接螺丝是否牢固，视情况进行紧固	1 次/季度
8	过滤网	检查过滤网是否脏堵，视情况更换过滤网	1 次/季度
9	加热器	检查加热器是否工作正常，热保护器是否灵敏。	1 次/季度
10	电磁阀	检查电磁阀的启停功能是否正常	1 次/季度
11	膨胀阀检查	检查膨胀阀过热度检查是否在合理范围内，调整或更换。	1 次/季度
12	干燥过滤器	干燥过滤器堵塞检查，运行 2 年以上每年更换一个。	1 次/季度
13	给排水管路	检查有无渗漏、排水是否通畅，视情况进行冲洗	1 次/季度
14	冷冻油	检查压缩机冷冻油颜色酸度及杂质含量，定期更换冷冻油。	1 次/季度

2）UPS 维护保养工作内容

序号	项目	内容	频率
1	环境检查	检查机房环境是否对 UPS 系统造成运行影响，视情况进行处理	1 次/季度
2	运行情况检查与备份	检查报警信息	1 次/季度
3		检查主机、风扇、显示屏运行是否正常	1 次/季度
4		备份报警信息	1 次/季度
5	除尘与紧固	检查外部灰尘情况，视情况处理	1 次/季度
6		检查内部灰尘情况，视情况进行清扫除尘、更换过滤网	1 次/季度
7		通过红外测温装置检查端子螺栓、螺帽是否过热，视情况处理	1 次/季度
8		紧固端子螺栓、螺帽(年度清扫检修中进行)	1 次/季度
9	电气检查	检查系统参数设置是否正常	1 次/季度
10		仪器测量器件、电缆等有无过热情况，检查外观是否损坏	1 次/季度

11		检查滤波电容有无漏液情况	1 次/季度
12		仪器测量母线纹波电压是否正常	1 次/季度
13		检查 IGBT 的外观是否正常	1 次/季度
14		检查输出三相负载是否均衡	1 次/季度
15		检查并机系统环流情况(如有并机系统)	1 次/季度
16		检查 UPS 系统输入、输出断路器整定值是否适当	1 次/季度
17		检查整流器外观是否正常	1 次/季度
18		检查逆变器外观是否正常	1 次/季度
19		检查转换为旁路工作模式后 UPS 供电是否正常	1 次/季度
20	电放电测试	进行电池放电测试、UPS 切换测试，检测 UPS 运行状态	1 次/半年
注：UPS 的年度清扫检修需在 UPS 主机停电(或维修旁路模式)状态下进行，并做好应对方案			

4.2 项目技术支持服务要求

项目技术支持服务要求包括故障修复要求、技术咨询要求、专业设备要求、维保公司资质的要求、维护人员要求、备件库要求和其他要求。

1)故障修复要求

1.维保公司须定期对机房基础设施服务对象进行全面技术检查、维护及保养，并做详细检查记录，记录包含巡检单维修单年度维护报告。

2.故障修复指当设备出现故障时，维保公司须为我局提供硬件设备修复、备件更换及系统软件故障排除的服务。由此产生的费用全部由维保公司负责。

3.在整个维护服务保修期内，维保公司应提供 7X24 的故障修复服务。当设备发生故障时，故障远程预警能够第一时间发出告警提示，值班员应第一时间通知维保公司，并着手处置故障。若维护工程师无法单独解决的，应立即通知维保公司，维保公司应自接到故障通知 2 小时内派人到达现场，负责检测并排除故障。对当日无法解决的故障或故障设备将影响系统正常运行的，应提供代用设备或应急解决方案，并确保系统正常运行。维保公司负责相关零部件的更换及维修，直至恢复设备的正常使用。故障排除后，维保公司须出具故障处理报告，帮助甲方进行故障根源的分析和诊断，提出后续工作的改进措施。

4.对于不能快速修复的特殊故障，维保公司要能够提供机房应急保障设备。

5.维保公司应每年向招标人书面报送《机房异常情况及处置情况汇总表》，分析设备运转情况，归纳异常情况形成的原因，制定下一步整改措施。

2）技术咨询要求

1.维保公司应免费提供技术咨询服务，包括新产品新技术通报，软硬件技术咨询，系统改进意见，提供技术解决方案(如:重要割接操作事前方案等)，项目长远规划，研究解决技术难题。

2.维保公司须以书面形式告知甲方 7*24 小时的专用维保不限于服务电话、移动电话、电子邮件、传真等联系方式以及提供支持服务过程中需要甲方准备的设备信息(如产品序列号等)，用于受理故障报修，解答甲方的技术咨询问题。如联系方式有变动，投标人须提前以书面形式通知甲方。

3）专业设备要求

维保公司应具有行业领先的专业仪器仪表以及专业维修工具。

4）维保公司资质的要求

维保公司应具有专业的服务工程师团队，可对供 UPS 系统、空调系统等机房设施进行完整维护及必要的健康年度检查，并提供方案。

5）维护人员的要求

中标公司需指定 1 名项目经理作为此项目的主要负责人。

1、项目经理的职责包括但不限于以下内容:

（1）负责制定维护方案和协调资源以满足甲方机房项目的工作需求。

（2）负责制定维护服务计划，包括例行的技术巡检。

（3）负责应对突发事件的应急响应和人员组织以及事后报告。

（4）负责配合甲方做好基础环境类的应急演练。

（5）负责配合甲方在关键时间节点期间做好应急保障工作。

★ 2、项目经理应满足以下要求:

（1）必须为维保公司的自有人员，提供近六个月的社会保险缴纳证明材料。

（2）应全面掌握数据中心基础设施运维相关知识及各系统在数据中心中的风险要害关系，并具有相应工作经验。

（3）项目经理应充分了解数据中心的各类基础系统的基本信息及运行工况。

（4）项目经理应做好 24 小时的应急响应，处理紧急事件时确保 1 小时内到达。

3、对维护操作工程师的要求

（1）维护操作工程师职责包括但不限于以下内容:

①负责制定对故障设备的维修方案，提交甲方进行风险评估。

②按照经过审核通过的维修方案进行设备维修实施。

③维修工程师需做好 24 小时的应急响应，紧急情况需 1 小时内到达。

④甲方将定期或不定期对维保公司的服务质量进行内部考核。

（2）维护操作工程师技能应满足以下要求:

①所有系统的维护操作工程师维修及安装作业前需进行自我安全教育并有安全员现场监督。

②应熟练掌握所维修维护设备的基本原理、工作工况、常规故障的解决方案、应急故障的处理预案等维修相关知识，具有相应工作经验。

二、弱电智能化运维服务要求

1、服务要求：

1.1 驻场服务：要求按照运维的系统，提供专业的人员进行驻场服务，提供不少于 3 名现场驻场运维工程师。

★驻场运维人员具备计算机相关专业知识，有相关项目工作经验，提供学历证书复印件及驻场人员履历表，熟练掌握各项设备维修和问题处理技能。

具体如下：

（1）监控系统运维服务:至少提供固定驻场人员 1 名，包含全院监控系统安装、维修、调试与软件服务，运维服务期限：1 年。

（2）门禁系统运维服务:至少提供固定驻场人员 1 名，包含全院门禁系统安装、维修、调试与软件服务，运维服务期限：1 年。

（3）其他运维系统服务:至少提供固定驻场人员 1 名，包含综合布线、时钟、巡更、一键报警等系统运维服务，运维服务期限：1 年。

1.2、资产梳理：针对不同的运维的系统，进行招标人的资产梳理登记工作，做好 IT 资产台账登记工作，以便更好的开展运维服务工作。

★ 1.3、原厂工程师技术服务：在驻场运维工程师不能及时解决故障时，提供原厂技术工程师现场技术支持服务。要求技术支持服务，1 年各不少于 30 次。监控、门禁系统需有原厂开具的技术服务承诺函，加盖原厂商公章。

1.4、咨询服务：按照招标方弱电智能化及中长期信息规划提供咨询服务。

1.5、运维服务具体要求如下：

监控系统	1.前端系统日常运行维护服务：包括摄像头的日常维护、故障排查和修复等。 2.后端平台运行维护及统筹调度服务：包括平台软件及服务端的更新、维护以及调度系统的优化等。 3.网络链路运行维护服务：确保视频数据传输的稳定性。 4.易损件与备品备件管理服务：确保系统各部件的及时更换和维护。 5.至少提供固定驻场人员 1 名，包含 5 个新装服务（包含硬件及线材），以及监控系统安装、维修、调试与软件服务。
门禁系统	1.前端设备 （1）读卡器：对读卡器刷卡的灵敏度进行测试。 （2）可视呼叫：对可视呼叫设备进行测试。 （3）人脸识别：对人脸识别设备进行测试。 （4）单元保护器：单元保护器对读卡器、电磁锁之间的电源电压是否正常。 （5）联网控制器：联网功能正常调节，测试与服务器通讯是否正常。 （6）门磁、门吸：是否能够正常关闭，正常吸合。 2.传输系统 （1）信号传输线路：线路连接状态，信号传输衰减，绝缘电阻大小，有无线路干扰，有无氧化。 3.监控中心 （1）中心主机：联网通信测试，保障通信正常。 （2） 通信器：工作状态是否正常。 4.包括门禁系统的维护和保养工作，确保系统及服务端的安全、可靠运行。具体服务范围可能包括设备检查、维修、保养、软件更新、故障排除等。 5.至少提供固定驻场人员 1 名，包含 10 个新装服务（包含硬件及线材），以及门禁系统维修、调试与软件服务。
其它系统	1.综合布线系统 （1）清除机柜内外综合布线系统上的灰尘。 （2）检查综合布线桥架的平整度，如果发生变形、支架螺丝脱落等与安装图纸不相符合的情况应立即修复。以免桥架断裂或脱落致使信息业务突然中断。 （3）检查双绞线上、面板上、配线架、跳线上的标签，将脱落的标签补全，将粘连不牢的标签固定好，更换有损伤的标签。 （4）使用性能测试仪对铜缆信道和未使用的光纤信道进行抽检，测试方法为永久链路测试和所用跳线的性能测试，并与原始记录进行核对。 （5）维护与保养：对易损部件进行定期检查和维护，如网线等易老化部件，一旦发现老化现象应及时更换或维修。 2.时钟系统 （1）定期对机房母钟进行巡检，查看授时方式是否改变，天线是否连接正常，多种授时方式是否均处在可用状态；定期巡检招标人单位场所的子钟运行情况，是否有损坏的显示单元，发现问题及时维修。 3.巡更系统

	（1） 系统检查 i.定期检查：定期对各个子系统进行检查，确保所有功能正常运行。这包括能源管理、环境监测、安全管理、设备管理等方面。 ii.故障诊断：对系统中发现的任何异常或故障进行及时诊断和处理，以防止小问题演变成大问题。 （2）软硬件维护 i.软件更新：定期更新系统软件，包括操作系统、应用程序和安全补丁，以确保系统的稳定性和安全性。 ii.硬件检查：对系统的服务器、监视平台、监控服务器和协议转换网关等硬件设备进行定期检查和维护。 （3）数据管理 i.数据备份：定期备份系统中的关键数据，包括配置设置、历史记录和报警日志，以防数据丢失。 ii.数据分析：对收集到的数据进行分析，以优化建筑设备的运行效率和能源消耗。 （4）安全管理 i.安全监控：定期检查安全监控系统，包括火灾报警、入侵检测和视频监控，确保其正常运行。 ii.访问控制：检查和维护门禁系统，确保只有授权人员能够访问关键区域。 （5）环境监测 环境参数：监测建筑物内外的环境参数，如温度、湿度、空气质量等，确保内部环境的舒适性和健康性。 （6）能源管理 能源消耗：监测和分析建筑物的能源消耗，通过调整照明、空调、供暖等设备的运行策略来优化能源利用。 （7）设备管理 设备状态：监测各种设备的运行状态，如电梯、空调、照明等，通过远程监控和管理提高设备的可靠性。 （8） 维护管理 i.预防性维护：根据设备的累计运行工况，提醒进行设备维护，以避免故障的发生。 ii.维护记录：记录所有维护活动，包括时间、内容和结果，以便未来参考。 4.一键报警系统 （1）定期检查：包括检查主机和探头的工作状态，确保正常运行；检查电源和线路，确保供电正常；检查报警器工作状态，确保报警准确；检查控制面板和软件界面，确保操作方便。 （2）设备保养：定期清洁设备表面，保持清洁干燥；定期更换电池，确保设备持续工作；定期检查探头灵敏度，确保准确报警；定期保养报警器，确保性能稳定。 （3）应急演练：定期组织员工进行应急疏散演练，提高员工安全意识；定期组织消防演习，提高员工灭火技能；定期检查消防设施是否完好，确保应急使用方便；定期检查报警系统是否正常工作，确保在火灾发生时能够及时报警。 （4）其他服务：协助招标人进行定期备份数据，确保系统数据安全；定期

	维护保养报警系统相关设备，确保性能稳定；发现异常情况及时处理，并上报相关负责人。 5.至少提供固定驻场人员 1 名，包含综合布线、时钟、巡更、一键报警等系统及服务。
备品备件及其他服务	1.提供监控系统常见备件和易损件更换服务，如：监控电源等。 2.提供门禁系统常见备件和易损件免费更换服务，如：门禁电源、门禁卡、门禁开关、磁力锁等。 3.提供综合布线系统常见备件和易损件免费更换服务，如网线、水晶头、配线架、理线架等，且提供 1 年不多于 100 点信息点位的综合布线施工（包含线材）。 4.运维过程中发现的其他故障问题，主要零部件，由双方协商另行采购，费用由招标人承担。

2.运维人员管理要求：

（1）运维工程师在提供服务期间需接受招标方管理，服从招标方工作安排，严格遵守招标方的各项管理及规章制；招标方对运维工程师进行考核、监督及评价。如需更换驻场工程师，须征得招标方同意方可。

（2）服务期内，双方须签订保密协议，供应商须严格保护招标方系统、数据、信息的安全，不得泄露服务过程中获取的敏感信息。由于供应商违反保密协议而导致的泄密或给招标方造成损失的，由供应商负全责，并由供应商赔偿招标方所有损失；构成犯罪的，移交司法机关处理。

（3）服务期内，供应商对运维人员财物或人身受到损害的事故负责。

3.服务方式：

（1）提供 7*24 小时服务，随时电话畅通。

（2）提供现场驻场服务，工作时间按照要求执行。

（3）提供应急保障服务，在重大任务期间或关键时间，要求提供 7*24 小时不间断现场值守服务。

（4）提供原厂技术支持服务，能够随时协助驻场人员处理问题，必要时能够上门服务。

★以上内容投标人须提供服务承诺函。

4.响应要求：

（1）接到服务请求后，驻场人员立即现场处理。

（2）驻场人员无法解决故障时，原厂技术工程师须在 2 小时内到达现场，并立即开始不间断现场支持。

（3）一旦定位是硬件故障，应在 1 小时内将原厂正品备件先行运抵现场，保证故障部件得到及时更换，使业务能在最短时间内恢复正常。

不同级别故障，分别承诺不同的解决时限。

故障级别	故障描述	解决时限
一级故障	系统瘫痪、设备无法运行或网络中断，影响生产经营活动正常运行的故障。	2 小时
二级故障	现有设备的操作性能严重下降，或由于设备性能明显下降，使最终的业务运作重要影响。	6 小时
三级故障	设备的操作性能受损，但大部分业务运作仍可正常工作	12 小时
四级故障	在产品功能安装或配置方面需要信息或支援，对业务系统几	24 小时

	乎无影响	

包 5：服务器存储维保服务

1、维护的要求和期限

（1）提供原厂软、硬件基本维保服务，包含但不限于提供原厂服务器、服务器虚拟化系统、存储设备技术的现场服务，硬件原厂备件更换现场服务，硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决招标人核心业务网设备故障、排除运行隐患，保证招标人各项业务的稳定运行。如提供非原厂服务，招标人有权拒绝选择投标人及拒绝与之签订合同、支付对应款项。

（2）维护期限：自合同签订之日起1年。

2、维护工作范围

★（1）投标人为采购人服务器、服务器虚拟化系统、存储设备提供 1 年产品可溯源原厂维保服务；服务标准为 7x24 小时级别，参保设备维护期限为 1 年，自合同签订之日起。

★（2）投标人应提供维保清单内具有满足本项目采购需求的一年售后服务的证明文件，包括但不限于售后服务承诺函或授权函等。

（3）负责本次招标所有系统设备的技术支持和运行维护工作。

3、维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助招标人技术支持人员维护网络稳定运行，满足招标人对高效、稳定的网络环境的需求。

（1）服务器、服务器虚拟化系统、存储设备及系统参保须为原厂保修：中标公司需确保招标方所要求维保服务清单内设备软、硬件更换为原厂可溯源保修或备件。

（2）客户服务经理与支持团队：在设备维保期内，原厂商指定专责服务主管、专责工程师团队；投标人须指定专职项目经理，项目经理的更换须得到招标人同意。

★（3）快速备件先行更换服务：投标人应向采购人提供及时周到的产品可溯源的快速备件更换服务。服务标准为备件先行7×24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂商正品备件先行运抵现场，保证故障部件得到及时更换，以使招标人的业务能在最短时间内恢复正常。

★（4）工程师快速现场支持服务：考虑到招标人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

A.工程师快速现场支持到达现场支持；

B.现场备件更换支持服务；

C.现场故障诊断及故障排除；

D.现场软件升级。

投标人工程师及投标人安排的原厂支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以招标人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，招标人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障－－设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间:1小时，故障排除时间≤8小时。

P2级故障－－设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障－－设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障－－咨询类问题或设备在运行安装过程中，客户对产品功能 配置等方面需要的信息和需求，对业务系统几乎无影响。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7×24的服务热线，由专门受理客户问题的维护团提供全天候无间断的产品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备的主机软件（COMWARE）的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明：为招标人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在招标人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出

安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地保证招标人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

★（8）巡检服务

原厂工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题，投标文件中需提供团队人员名单，相应证书，劳动合同关键页及原厂商为工程师缴纳社保证明。

（9）重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与招标人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从招标人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合招标人做好内网电脑入网、可受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。招标人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

★ 7、驻场人员要求

服务期内，投标人需要提供 1 名工程师进行驻场服务。驻场工程师要求有三年以上 IT 设备运维工作经验，具备厂商中级及以上认证证书（或具体同等能力水平）。具体工作包括以下内容：

A.日常设备维护。精通数据中心常见服务器（如 HPE、新华三、华为、联想、浪潮等）设备的日常运维、巡检、故障定位与处置能力，精通服务器虚拟化软件 CAS、VMware 的日常

运维运维、巡检、故障定位与处置能力，具备本次招标涉及的设备及系统的日常运维能力，必要时能够进行调整和优化，保障平台正常运行；

B.补丁、版本升级服务。能够对数据中心各项服务器及虚拟化系统进行软件补丁、版本升级，使数据中心各项设备处于良好运行状态；

C.故障处理。预警并协助数据中心预防重大故障的发生，在发生故障时可以快速解决故障；

D.保障服务。为了保障重大节日期间机房软硬件支撑环境安全运行，向招标人提供现场工程师值守服务，并在保障结束后提供服务总结报告和建议；

E.其他现场技术支持服务。包括相关技术咨询、新需求的配合解决、 配合割接实施等其他现场技术支持服务。

8、IT 设备性能提升服务

★投标人需针对续保清单中存储服务器设备开展性能优化：考虑医院业务的重要性，要求实施人员为原设备生产厂商技术工程师，投标文件中需提供团队人员名单，相应证书，劳动合同关键页及原厂商为工程师缴纳社保证明。

本次项目交付针对现场存储、服务器等设备进行排查，输出性能提升方案，并进行优化整改。包含不限于设备业务统计、CPU 及内存使用情况、虚拟化资源分配情况摸排等，并根据实际情况输出优化方案，优化资源分配等工作

9、维保服务清单

序号	设备名称	设备型号	产品描述	数量
1	备份软件	CB	H3C CB 备份软件	1
2	虚拟带库	Storeonce 5100	HPE StoreOnce 5100 48TB	2
3	全闪存阵列	3PAR 8450	HPE 3PAR 8450 4N+SW Storage Field Base	2
4	集中存储	3PAR 8200	HPE 3PAR 8200 2N+SW Storage Field Base	1
5	物理带库	MSL4048	HP MSL4048 物理带库	1
6	HPE	SN3600B	HPE SN3600B 32Gb 24/24 FC Switch	2
7	集中存储	3PAR SS8400	HPE 3PAR 8400 2N+SW Storage Field Base	1
8	备份一体机	ST-CB3024	H3C UniStor CB3024 备份一体机 (2*550W AC,2U,64GB 内存,标配 24TB,可扩展到 48TB)	1
9	外网存储	外网 IP SAN 存储	CF8820	1
10	业务存储	MSA2040	MSA2040 存储设备	2

11	存储交换机	SN6000B	SN6000B 光交换机	4
12	刀片服务器机箱	Bladesystem C7000	HPE BLc7000 1PH 2PS 4Fan Trl IC Plat Encl	2
13	虚拟化服务器	BL460c	HPE BL460c 刀片式服务器	30
14	管理服务器	BL460c	HPE BL460c 刀片式服务器	2
15	服务器虚拟化系统	VC-CAS-ENT	功能模块-H3C CAS-VCAM8CAS-CAS 云计算管理平台-纯软件(DVD)-国内版	1
16		LIS-CAS-CVMA-ENT-2	License 授权函-H3C CAS-VCAM8CVMA-CVM 虚拟化管理系统企业版软件 License 费用-管理 2 个物理 CPU-国内版	30
17	HIS 业务备份服务器	DL580 Gen9	HPE DL580 GEN9 服务器	2
18	日志采集与分析系统	RS-FD4530-21SFF-ITOA	装配组件-H3C FlexData 4530-RSBZ1FD4530-4U 服务器-国内海外合一版	1
19	关键业务数据库服务器	HPE Superdome X	HPE Superdome X Base Enclosure	2
20	虚拟化服务器	UIS-R690-G2-5SFF-C	H3C UIS R690 G2 5SFF CTO 服务器(CPMO)	4
21	计算服务器	UIS-R390X-G2-8SFF-C-A	H3C UIS R390X G2 8SFF CTO 服务器(含导轨、安全面板)	3

包 6：网络安全维保服务

1、维护的要求和期限

（1）提供原厂软、硬件基本维保服务，包含但不限于提供原厂网络、安全设备及网管系统技术现场服务，硬件原厂备件更换现场服务，硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决招标人核心业务网设备故障、排除运行隐患，保证招标人各项业务的稳定运行。如提供非原厂服务，招标人有权拒绝选择投标人及拒绝与之签订合同、支付对应款项。

（2）维护期限：自合同签订之日起1年。

2、 维护工作范围

★（1）投标人为采购人网络、安全设备及网管系统提供 1 年产品可溯源原厂维保服务；服务标准为 7x24 小时级别，参保设备维护期限为 1 年，自合同签订之日起。

★（2）投标人应提供维保清单内具有满足本项目采购需求的一年售后服务的证明文件，包括但不限于售后服务承诺函或授权函等。

（3）负责本次招标所有系统设备的技术支持和运行维护工作。

3、 维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助招标人技术支持人员维护网络稳定运行，满足

招标人对高效、稳定的网络环境的需求。

（1）网络、安全设备及网管系统：中标人需确保本次招标所有系统设备参保设备软、硬件更换为原厂保修或原厂备件

（2）客户服务经理与支持团队：在设备维保期内，原厂商指定专责服务主管、专责工程师团队；投标人须指定专职项目经理，项目经理的更换须得到招标人同意。

★（3）快速备件先行更换服务：投标人应向采购人提供及时周到的产品可溯源原厂的快速备件更换服务。服务标准为备件先行7×24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂商正品备件先行运抵现场，保证故障部件得到及时更换，以使招标人的业务能在最短时间内恢复正常。

★（4）工程师快速现场支持服务：考虑到招标人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

A.工程师快速现场支持到达现场支持；

B.现场备件更换支持服务；

C.现场故障诊断及故障排除；

D.现场软件升级。

投标人工程师及投标人安排的原厂支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以招标人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，招标人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障－－设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间:1小时，故障排除时间≤8小时。

P2级故障－－设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障－－设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障－－咨询类问题或设备在运行安装过程中，客户对产品功能 配置等方面需要的信息和需求，对业务系统几乎无影响。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7×24的服务热线，由专门受理客户问题的维护团提供全天候无间断的产

品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备的主机软件的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明:为招标人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在招标人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地保证招标人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

★（8）巡检服务

原厂工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题。

（9）重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与招标人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从招标人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合招标人做好内网电脑入网、可受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。招标人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实

施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

★ 7、驻场人员要求

（1）网络运维驻场服务

序号	具体要求
1	网络运维人员驻场服务（1 人）： （1）服务期内，投标人需要提供 1 名网络工程师进行驻场服务。驻场工程师要求有三年以上网络设备运维工作经验，具备厂商中级及以上认证证书（或具体同等能力水平）。具体工作包括以下内容： A.日常设备维护。精通常见网络设备（如：华为、新华三、锐捷、思科等）日常运维、巡检、故障定位与处置能力，精通网管软件日常运维、巡检、故障定位与处置能力，具备本次招标涉及的设备及系统的日常运维能力，必要时能够进行调整和优化，保障平台正常运行； B.补丁、版本升级服务。及时对招标人网络设备及网管软件进行软件补丁、版本升级，使数据中心各项设备处于良好运行状态； C.故障处理。预警并协助数据中心预防重大故障的发生，在发生故障时可以快速解决故障； D.保障服务。为了保障重大节日期间机房软硬件支撑环境安全运行，向我方提供现场工程师值守服务，并在保障结束后提供服务总结报告和建议； E.其他现场技术支持服务。包括相关技术咨询、新需求的配合解决、 配合割接实施等其他现场技术支持服务；

（2）安全运维驻场服务

序号	具体要求
1	安全运维人员驻场服务（2 人）： 按招标人作息时间上下班，通过专业技术手段落地可持续安全运营体系，围绕预测与发现、监测与分析、防御与控制、响应与管理形成的安全闭环，切实解决我院信息安全问题。所提供安全运营中心工具能够与不少于 3 个系统的防火墙进行联动，自动下发安全策略，以提高应急响应效率。服务内容如下： 安全资产管理服务： ● 对在网资产进行自发现和手动添加，配合安全运营中心态势监控功能，集中统一维护，对内网资产进行全方面的监测。

	● 采用检查用表（checklist）定期对评估目标范围内的主机系统安全、中间件安全、数据库安全等进行系统的安全规则配置、安全策略配置、日志报警信息以及系统和软件升级、更新情况，是否存在后门等内容进行检查。 脆弱性评估服务： ● 在服务期内持续发现环境中存在的 web 应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露等脆弱性问题，针对扫描结果进行人工验证并去除误报，生成相关报告并提供加固建议。 ● 原厂安全服务工程师对脆弱性评估结果进行人工验证，保证脆弱性评估报告的真实性。 ● 提交针对性的解决方案，保证漏洞修复可落地。 日志分析服务： ● 原厂安全服务工程师基于状态与行为的威胁事件检测和分析引擎，结合大数据架构集中存储的网络流量数据、安全设备和主机日志，以及外部威胁情报信息。综合多种信息元素进行全局网络的流量分析、日志分析及关联分析，深度挖掘潜在的威胁行为,还原攻击路径，发现攻击意图。 ● 定期提取威胁日志数据进行安全分析，对系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结，查找潜在的攻击痕迹，分析日志当中真实存在威胁以及病毒或木马攻击痕迹，找出确定有效的攻击，并交付日志分析报告。 风险管理服务： ● 原厂安全服务工程师梳理终端、服务器和外网三者之间内到内、内到外、外到内之间的威胁互访关系，实现追踪攻击路径，定位攻击源，预测攻击面； ● 对安全运营中心发现的异常行为威胁事件进行提取及呈现； ● 提供所有 IOC 威胁事件分类统计和两周内威胁事件的趋势变化； ● 通过对威胁事件的分析，提炼威胁事件的核心内容及影响，使专业的威胁事件转化为简单通俗易懂的描述，便于用户分析威胁事件的影响及内容。 安全培训服务： ★ **服务要求：**驻场工程师（至少一名）具备开展信息安全意识、安全攻防技术及安全认证等方面培训的能力。要求驻场工程师具备 CISP（注册信息安全专业人员）类证书，并具备 CNVD（中国国家漏洞库）认证，具有参与 CTF（Capture The Flag）网络安全竞赛的经验,至少在一家知名安全厂商工作过,有大型甲方安全服务经验，并参与过国家级的网络安全专项行动。 服务周期：1 年。 服务交付物:《安全运营报告》
2	安全事件应急服务： **服务内容：**提供安全事件应急响应工作。在在出现重要安全事件时（信息系统遭受攻击、网络病毒爆发等），派遣高级安服人员，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等，协助用户解决突发安全事件，并提供应急响应报告。 **服务要求：**当发生信息安全事件时，专业工程师须 10 分钟内响应并在 30 分钟内到

	达现场启动应急处置工作，提供安全事件处置、应急操作、安全加固建议，并协助相关部门处理安全问题；事件处置后提供事件分析处理报告，就安全风险、安全事件描述，危害性，原因、排查过程、处置加固方法等进行详细说明； **服务频率：**服务周期为 1 年，全年提供不限次数的安全应急响应服务。
3	安全预警通告服务： **服务内容：**以邮件、文件、电话等方式，将安全技术和安全信息及时传递给招标人，使招标人能保持对信息安全最新动态的认识，提前预知风险，每月末以邮件方式提交安全月报。安全通告内容至少包括：目前主流操作系统的安全漏洞补丁；信息安全业界最新动态与技术；国内外最新信息安全趋势；紧急安全事件通告；最新的国内、外行业安全政策及法律法规。 **服务频率：**服务周期为 1 年，提供全年不限次数安全通告服务。 交付物：《网络安全预警通告》
4	安全巡检服务： **服务内容：**服务工程师到现场进行安全巡检服务，对客户网络及重要服务器进行分析，主要包括网络、安全设备的配置检查，对网络和安全设备的运行状态、安全策略、漏洞库等进行安全配置核查；服务器配置核查，对服务器资源、身份鉴别、默认配置、共享设置、补丁管理、日志等进行安全配置核查；安全设备日志分析，检查防火墙、入侵检测和其他安全设备的日志信息，对其进行分析，排查网络中可能发生的安全事件；服务器木马查杀，发现存在木马、病毒等恶意程序，及时进行查杀清理，避免被不法分子利用进行后续横向扩散。 **服务交付物：**《安全巡检报告》
5	安全加固服务： **服务内容：**依据招标人的安全加固需求，对服务器、中间件、数据库、网络和安全设备提出系统加固的方案，确保系统的问题被修复或风险可控； **服务频率：**服务周期为 1 年，全年不限次数随时提供安全加固服务。 交付物：《安全加固建议方案》
6	系统上线前的安全检测： **服务内容：**针对新业务系统上线前，从主机层、系统层、数据库层、中间件层全面评估新系统的安全状况，查找不符合安全要求的配置项以及安全风险点。 **服务要求：**通过漏洞扫描、渗透测试、安全基线检查在内的安全评估服务手段，发现该业务系统存在安全隐患，并提出加固解决措施，协助开发单位进行整改。 **服务交付物：**《漏洞扫描报告》、《渗透测试报告》、《安全基线检查报告》 **服务频率：**服务周期为 1 年，全年提供不限次数的新系统上线检测服务。
7	资产梳理： **服务内容：**针对招标人内外网硬件资产、业务系统资产进行全方面梳理，深入发现未知的资产，缩小资产盲区。 **服务范围：**梳理对象包括但不限于：应用系统、数据库、安全设备、交换机、电脑终端、摄像头、打印机、服务器等。 **服务交付物：**《资产台账清单》、《网络安全拓扑图》
8	设备安全策略检查优化服务： **服务要求：**服务商需定期针对招标人安全设备包括：防火墙、入侵检测系统、网闸、WAF 等进行安全策略细化、调优服务。 **服务频率：**服务周期为 1 年，全年不限次数提供设备安全策略检查优化服务。 《网络安全策略优化报告》

8、渗透测试服务

技术项	具体要求
服务概述	渗透测试是为了证明招标人互联网服务的网络防御按照预期计划正常运行而提供的一种机制， 由安全专家模拟恶意黑客的攻击行为，通过远程方式对信息系统进行非破坏性的入侵测试。 这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析。渗透测试可以发现逻辑性更强、更深层次的漏洞，并直观反映漏洞的潜在危害，更加真实的了解到信息系统的安全性状况，为信息系统的安全配置与管理提供指导建议。
服务内容	1、针对招标人互联网服务进行全面测试，采用自动化工具及人工测试方法相结合，深度挖掘业务系统存在的安全漏洞，对系统的脆弱性进行分析。具体内容包括但不限于信息收集、端口扫描、漏洞检测、口令猜测、后门安全检查等。 2、提供整改建议，协助进行安全整改，经整改或加固后，渗透测试人员进行回归测试，即二次复测，复测结束后提交给招标人复测报告和对复测结果进行沟通。 3、每次渗透测试完成后，提供整理渗透测试服务输出成果，进行汇报。
服务流程	1、前期准备阶段 在实施渗透测试工作前，技术人员和用户对渗透测试服务相关的技术细节进行详细沟通。由此确认渗透测试的方案，方案内容主要包括确认的渗透测试范围、最终对象、测试方式、测试要求的时间等内容。 2、测试阶段实施 测试人员首先使用自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。然后由人工的方式对安全扫描的结果进行人工的确认和分析。并且根据收集的各类信息进行人工的进一步渗透测试深入。 结合自动化测试和人工测试两方的结果，测试人员需整理渗透测试服务的输出结果并编制渗透测试报告，最终提交用户和对报告内容进行沟通。 3、复测阶段实施 在经过第一次渗透测试报告提交和沟通后，等待用户针对渗透测试发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给用户复测报告和对复测结果进行沟通。 4、成果汇报阶段 根据一次渗透测试和二次复测结果，整理渗透测试服务输出成果，最后进行成果汇报。
服务频率	★ 服务周期为 1 年，一年内开展两次全面渗透测试，单次渗透测试的范围至少包含 20 个业务系统。
交付物	《渗透测试报告》
服务要求	★ 渗透测试服务工程师应熟悉和掌握不同的渗透测试工具和技术，拥有强大的漏洞挖掘与分析能力，具备安全评估与报告撰写能力，应具备 CISP、CISP-PTE、PMP 资格证书。

9、无线网络优化服务

★投标人需针对现有招标人无线网络覆盖优化：考虑内网业务的重要性，要求实施人员为原设备生产厂商技术工程师，投标文件中需提供团队人员名单，相应证书，劳动合同关键页及原厂商为工程师缴纳社保证明。

本次项目交付针对内网弱信号区域排查故障情况，输出优化方案，并进行优化整改。包含不限于现场使用情况调查、信号扫描、线路整改、AP安装位置调整、AP信道优化等，共计3轮测试、2轮优化。外网针对使用情况进行优化，保证招标人在院区内信号覆盖区域内正常接入及认证上线。

10、维保服务清单

序号	设备型号	设备类型	产品描述	数量
1	核心交换机S12508X	LSWM1QSTK2	功能模块-H3C S5820V2-LSWM1QSTK2-40G QSFP+电缆-5m-国内海外合一版	4
		PSR2400-54A	功能模块-H3C S12500X-AF-LSXM1PSRA-2400W交流电源模块-国内海外合一版	8
		LSXM1SUPB1	功能模块-H3C S12500X-AF-LSXM1SUPB1-主控制引擎模块-国内海外合一版	4
		LSXM108XFAN	功能模块-H3C S12508X-AF-LSXM108XFAN-以太网交换机风扇模块-国内海外合一版	4
		LSXM1IMA	功能模块-H3C S12500X-AF-LSXM1IMA-业务板适配器-国内版	4
		LSXM1GT48FX1	功能模块-H3C S12500-X-LSXM1GT48FX1-48端口千兆以太网电接口模块(RJ45)(FX)-国内版	2
		LSXM1TGS24FX1	功能模块-H3C S12500-X-LSXM1TGS24FX1-24端口万兆以太网光接口模块(SFP+,LC)(FX)-国内版	2
		LSXM1SFF08A1	功能模块-H3C S12508X-AF-LSXM1SFF08A1-交换网板-F型(A类)-国内版	12
		LS-12508X-AF	装配组件-H3C S12508X-AF-LSXZ108X-以太网交换机主机-国内海外合一版	2
2	外网核心交换机S10506	LSUM1MPU06B0	功能模块-H3C S10506-LSUM1MPU06B0-主控交换模块-国内版	2
		LSUM1FAB06C0	功能模块-H3C S10506-LSUM1FAB06C0-交换网板-C类-国内版	1
		LSUM2GT24PTSSE0	功能模块-H3C S10500-LSUM2GT24PTSSE0-24端口千兆以太网电接口(RJ45)+20端口千兆以太网光接口(SFP,LC)+4端口万兆以太网光接口模块(SFP+,LC)(SE)-国内海外合一版	1
		LSUM1TGS16FD0	功能模块-H3C S10500-LSUM1TGS16FD0-16端口万兆以太网光接口模块(SFP+,LC)(FD)-国内海外合一版	1
		LS-10506	装配组件-H3C S10506-LSUZ110506-以太网交换机主机-国内版	1
		LSUM1AC2500	功能模块-H3C S10500-LSUM1AC2500-2500W交流电源模块-国内海外合一版	2
3	核心交换机S10506	LSUM1FAB06C0	H3C S10506 交换网板,C类	2
		LSUM2TGS48SG0	H3C S10500 48端口万兆以太网光接口模块(SFP+,LC)(SG)	2
		LSUM1AC1200	交流电源模块,1200W	4

		LSUM1MPU06B0	H3C S10506 主控板,B 类	4
		LS-10506	H3C S10506 以太网交换机主机	2
4	汇聚交换机	LSPM2150A	150W 资产管理交流电源模块	1
		LSPM1FANSB	风扇模块(SW，4028,风扇面板侧出风)	2
		LS-5560X-30F-EI	H3C S5560X-30F-EI L3 以太网交换机主机(24SFP(8GE Combo)+4SFP Plus+1Slot),无电源	1
5	数据中心交换机	LSPM2150A	150W 资产管理交流电源模块	1
		LSPM1FANSB	风扇模块(SW，4028,风扇面板侧出风)	2
		LS-5560X-54C-EI	H3C S5560X-54C-EI L3 以太网交换机主机,支持 48 个 10/100/1000BASE-T 端口,支持 4 个 10G/1GBASE-X SFP+端口,支持 1 个 Slot,无电源	1
6	无线控制器	LSPM2150A	150W 资产管理交流电源模块	1
		EWP-WX3510H	H3C WX3510H 无线控制器	2
7	ACG1000	NS-SecPath ACG1000-X	数据通信-H3C SecPath ACG1000-X-应用控制网关主机(4GE Combo+3Slots)-国内版	1
		AC-PSR300-12A2	功能模块-H3C MSR-RTUM1PWR300A-300W AC 电源模块-国内版	2
		NSQM1TGS4	数据通信-H3C SecPath ACG1000-E-4 端口万兆以太网模块(SFP+)接口卡-国内版	1
8	S10510	LS-10510	装配组件-H3C S10510-LSUZ110510-以太网交换机主机-国内版	2
		LSUM1TGS24FD0	功能模块-H3C S10500-LSUM1TGS24FD0-24 端口万兆以太网光接口模块(SFP+,LC)(FD)-国内海外合一版	3
		LSUM1FAB10C0	功能模块-H3C S10510-LSUM1FAB10C0-交换网板-C 类-国内版	4
		LSUM1MPU10C0	功能模块-H3C S10510-LSUM1MPU10C0-主控交换模块-国内版	4
		LSUM1AC2500	功能模块-H3C S10500-LSUM1AC2500-2500W 交流电源模块-国内海外合一版	4
9	认证网关 WX5540H	EWP-WX5540H	装配组件-H3C WX5540H-EWPXZ15540H-无线控制器主机(12GE+12SFP+4SFP Plus)-国内海外合一版	1
		LSPM2150A	150W 资产管理交流电源模块	2
10	7506E	LS-7506E-NonPoE	装配组件-H3C S7506E-LSQZ17506ENP-以太网交换机主机-非 PoE-国内版	1
		LSQM3MPUB0	功能模块-H3C S7506E-NonPoE-LSQM3MPUB0-主控交换模块-国内海外合一版	2
		LSQM1AC650C	以太网交换机交流电源模块-650W	2
		LSQM2GT24PTSSC0	功能模块-H3C S7500E-LSQM2GT24PTSSC0-24 端口千兆以太网电接口(RJ45)+20 端口千兆以太网光接口(SFP,LC)＋4 端口万兆以太网光接口模块(SFP+,LC)(SC)-国内海外合一版	1
11	终端准入	SWP-IMC7-IMP	H3C iMC-智能管理平台标准版，医院内网和外网各一套，外网包含 EIA 准入模块	2 套

	与管理系统			
12	接入交换机	LS-5130S-28P-HPWR-EI	数据通信-H3C S5130S-28P-HPWR-EI-LS5Z1S28PHPE-L2 以太网交换机主机(24GE(PoE+)+4SFP+4GE Combo)-(AC/DC)-国内版	38
13	网络优化	无线网络优化服务	现有全院无线网络覆盖优化： 考虑内网业务的重要性，本次项目交付针对弱信号区域排查故障情况，输出优化方案，并进行优化整改。包含不限于现场使用情况调查、信号扫描、线路整改、AP 安装位置调整、AP 信道优化等，共计 3 轮测试、2 轮优化。	1
14	态势感知平台升级服务	SG-6000-1SC6220	★ 1、现有态势感知平台升级，提供不少于 7 类情报库，包括 DNS 类、恶意代码类、URL 类、IP 类、弱点类、入侵检测类、地理库。 2、支持对第三方设备的 Syslog 日志进行解析、呈现，并做进一步分析；针对常见的第三方网络安全设备，提供了预定义日志解析配置及模板；同时也支持根据 Syslog 日志信息的格式，创建自定义的日志解析配置及模板，解析规则包括 Grok 解析、Key-Value 解析、JSON 解析。 3、支持总览现网安全态势，包括综合评分、威胁攻击分布、热点事件、资产风险状况、最新安全事件、弱点态势。 4、支持勒索类规则，根据勒索软件行为进行分析和检测，支持挖矿类规则，智能检测挖矿行为特征。 ★5、提供不少于一年原厂售后服务和不少于一年特征库升级服务，含配套软件、辅材、安装调试等。	1
15	探针升级服务	（BDS-12830-ThreatSensor）	★1、现有探针（BDS-12830-ThreatSensor）升级，升级后功能符合《河南省卫生健康行业网络安全态势感知数据采集规范（试行版）》，可以将相关安全数据对接上传至河南省卫生健康行业网络安全一体化监管服务平台，且质量达标。 2、支持流量基线自学习功能，配置低/中/高三级检测灵敏度，配置 7-28 天的流量学习周期，自动创建流量基线。 3、支持异常行为类攻击检测，至少包括扫描攻击检测、恶意完整访问检测、SMB NETBIOS 逃逸检测、可疑 NETBIOS 行为检测、SMB 端口扫描检测、暴力破解检测、DNS 域名被劫持检测、比特币挖矿行为检测等。 ★ 4、提供不少于一年原厂售后服务和不少于一年特征库升级服务，含配套软件、辅材、安装调试等。	1

16	威胁感知设备升级服务	BDS-I2850	1、现有威胁感知设备升级。 2、应用识别、入侵攻击检测、病毒检测、未知威胁检测特征库的升级。 支持基于高级威胁行为集的未知威胁检测 3、支持大于 2000 种高级恶意软件家族的检测，包含 Virus、Worm、Trojan、Over ow 等类型. 4、支持基于建立电脑和服务器行为数据模型的异常行为检测 5、支持 HTTP 扫描、Spider、SPAM、SSH/FTP 弱口令等异常行为的检测 6、支持精准定位失陷电脑及风险服务器，通过证据报文溯源攻击细节。 ★7、提供不少于一年原厂售后服务和不少于一年特征库升级服务含配套软件、辅材、安装调试等。	1
17	外网防火墙续保服务	SG-6000-E5560	1、现有出口防火墙（SG-6000-E5560）续保服务。 2、源 NAT 模式下，支持将每一个源 IP 地址所产生的所有会话都转换到同一个固定的外部 IP 地址上； 3、支持 NAT 转换扩展技术，使每个 IP 地址支持的 NAT 转换端口突破 65535 端口的限制； 4、支持通过 ping、tcp、dns 等方式进行链路有效性探测，可根据探测结果使相应接口关闭和路由信息失效； 5、支持通过 ping、tcp、dns 等方式进行 NAT 探测，支持基于指定源 IP 进行探测，支持对 NAT 转换后的地址是否有效进行探测； ★6、提供不少于一年原厂售后服务和不少于一年特征库升级服务含配套软件、辅材、安装调试等。	1

三、方案要求

序号	要求款项	要求内容	备注信息
1	项目需求理解	提供项目需求理解方案	
2	项目组织架构	提供项目组织构架方案	
3	应急方案响应计划	提供应急方案响应计划	
4	确保服务质量措施	提供服务质量措施	