

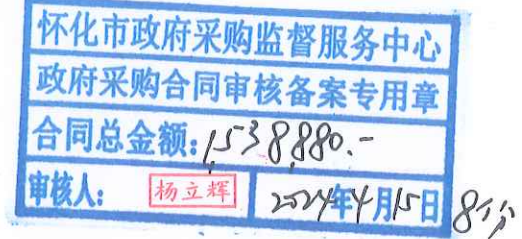
政府采购合同

第一节 政府采购合同协议书

采购合同编号：2024HCZB 020

采购人（甲方）（全称）：怀化市第二人民医院

供应商（乙方）（全称）：湖南华众时代信息技术有限公司



为了保护甲、乙双方合法权益，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及其他有关法律、法规、规章，双方签订本合同协议书。

1. 项目信息

(1) 采购项目名称：怀化市第二人民医院 PACS 基础设施硬件采购和网络安全类设备采购

(2) 采购计划编号：怀财采计 202410006

(3) 采购项目包号及名称：02 包、网络安全类设备采购

(4) 项目内容：

设备名称		规格型号	设备参数	品牌/产地	数量/单位	金额（元）		备注
						单价	小计	
1	零信任综合网关（核心产品）	aTrust-1000-B103OM-AK	1、最大加密流量 300Mbps，最大并发用户数 400，最大 https 并发连接数 15000，https 新建连接数（个 /秒） 60。零信任接入授权 50 个。网络接口：千兆电口 6 个，千兆光口 2 个。提供不少于三年硬件质保及软件免费升级服务。 2、支持基于 TCP、UDP、ICMP 等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等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。 3、支持基于 http 或 https 协议代理访问业务资源，支持发布 IP 或域名形式的后端服务器地址，可配置业务应用的具体访问 URL 路径。为了保持用户访问应用体验的一致性，后端服务器地址	深信服/深圳	1 台	80000	80000	

		<p>需支持多地址配置；为 适应较复杂的内外网访问场景，WEB 应用的前端访问地址应支持多地址访问。</p> <p>4、支持配置应用资源指定的打开方式，如浏览器等；为了适应某些业务系统对浏览器的兼容性，还应支持 配置应用打开的指定浏览器类型。</p> <p>5、WEB 资源发布时应支持到 URL 路径级别，且支持配置 URL 路径规则。黑名单模式下，用户只能访问不在黑名单内的路径；白名单模式下，用户只能访问白名单内的路径。</p> <p>6、支持以下认证方式：本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议 的票据认证、Radius 账号认证、HTTPS 帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标 准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书 结合实现扫码认证，支持飞书用户或个人微信企业号通过 H5 接入。其中短信认证支持配置 HTTPS 短信网关、腾讯云短信网关、阿里云短信网关及 Socket 短信网关等网关类型。</p> <p>7、支持帐号密码代填的单点登录功能，支持智能识别登录页面的用户名和密码输入框，根据设置的用户名 密码规则自动填写 WEB 业务系统的帐号密码并登录；支持精准识别的代填模式，以业务登录界面的帐号输入 框、密码输入框、登录按钮等作为匹配项，自定义精确匹配零信任用户名、密码、组织架构名、手机号、邮 箱、邮箱前缀等值，也可以设置由终端用户自定义输入或管理员设定固定值登录。</p> <p>8、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。</p> <p>9、支持单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描</p>				
--	--	--	--	--	--	--

			<p>到服务端口，不会出现敲门放大漏洞。</p> <p>10、支持跟院方现有桌面云进行单点登录对接，实现仅需在零信任进行认证即可直接进入云桌面进行业务办公，无需重复验证，提高桌面云远程访问时的安全性。</p> <p>11、支持将流量日志对接院内威胁感知探针解密分析，确保流量分析全面。</p>				
2	终端检测与响应	<p>端点安全软件 V3.0 (PC 基础版)</p>	<p>1、PC 终端授权，整体提供 2 套终端检测响应平台软件产品控制中心，提供不少于三年软件升级服务和安全 规则库更新服务。</p> <p>2、支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门、高危漏洞及其各自影响的终端数量。</p> <p>3、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户。</p> <p>4、基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。</p> <p>5、一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。</p> <p>6、支持流行 Windows 高危漏洞的轻补丁免疫防御，支持 Windows 补丁批量一键修复。</p> <p>7、支持自定义拦截终端软件弹窗，可在终端设置自动拦截骚扰弹窗开关。</p> <p>8、支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。</p> <p>9、支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内</p>	深信服/深圳	1600 套	129	206400

			<p>容、攻击历史。</p> <p>10、支持与我院现有态势感知平台进行安全联动，支持管理员在安全感知管理平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置。</p> <p>11、支持与我院现有互联网出口防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。</p> <p>12、支持安全日志上报我院现有 MSS 服务管理平台对接，进行联合分析溯源终端威胁事件并联动响应。</p> <p>13、支持与本次项目购买的零信任综合网关联动，将资产信息同步零信任综合网关（零信任综合网关），以完善零信任综合网关（零信任综合网关）资产管理与测绘能力。</p>					
3	高性能防火墙	AF-2000-FH2250B-MF	<p>1、网络层吞吐量 35Gbps，应用层吞吐量 20Gbps，并发连接数 410 万，每秒新建连接数 18 万，电源：冗余电源，网络接口数：千兆电口 16 个，万兆光口 6 个，配置 10 块万兆多模-850-300m-双纤。含 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、WEB 应用防护模块、防病毒模块，提供三年硬件质保及软件升级和 WEB 应用防护识别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL&应用识别库更新服务。</p> <p>2、支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT 等资源。</p> <p>3、支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式。</p> <p>4、支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。</p> <p>5、支持对压缩病毒文件进行检测和拦</p>	深信服/深圳	2 台	150000	300000	

			<p>截，压缩层数支持 15 层及以上。</p> <p>6、支持勒索病毒检测与防御功能。</p> <p>7、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。</p> <p>8、支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封 锁高危 IP。</p> <p>9、支持与本院现有态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。</p> <p>10、支持与本院现有服务器 EDR 联动管理，在防火墙产品完成服务器杀毒软件的统一管理。支持检测到某主机有僵木蠕毒的 C2 通信时，手动或自动化将恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文 件进行隔离。</p>					
4	网管平台	SdSec-1000-WG200	<p>1、提供 200 个资产管理授权。提供三年软件升级服务。</p> <p>2、支持从备份文件恢复某个时间点的数据，支持备份文件直接恢复为数据库。恢复完成验证可用性验证后 可以替换原有业务作为现使用业务。</p> <p>3、支持手动巡检与自动巡检，并生成巡检报告，巡检报告可提供健康评分。</p> <p>4、支持多级租户模型，包括平台管理员、租户账号界面，各自具备不同的数据库资源使用范围及权限。</p> <p>5、支持提供数据库监控大屏，提供数据库故障定位、异常问题汇总、TOP 统计等。</p> <p>6、支持对数据库实例进行监控，并根据监控展示趋势图，提供 10+监控指标。</p>	深信服/深圳	1 套	118200	118200	
5	专线防火墙	AF-2000-FH2250B-F5	<p>1、网络层吞吐量 35Gbps，应用层吞吐量 20Gbps，并发连接数 410 万，每秒新建连接数 18 万，电源：冗 余电源，网络接口数：千兆电口 16 个，万兆光口 6 个，配置 4 块万兆多模-850-300m-双纤。含 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测，提供三年硬件质保及软件升级和 WEB 应用防护识</p>	深信服/深圳	2 台	104250	208500	

		<p>别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL&应用识别库更新服务。</p> <p>2、支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>3、支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>4、支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀。</p> <p>5、支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>6、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息。</p> <p>7、支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面</p> <p>8、支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP。</p> <p>9、支持与本院现有态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。</p> <p>10、支持与本院现有服务器杀毒安全软件联动管理，在防火墙产品完成终端安全策略设置和服务器杀毒软件的统一管理，支持检测到某主机有僵尸蠕毒的 C2 通信时，手动或自动化将恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离。</p> <p>11、为保障后续三院数据融合后安全统</p>				
--	--	--	--	--	--	--

			一运维管理，满足设备安全联动。实现安全事件的发现-分析-处置 闭环，本次项目中要求终端检测与响应、高性能防火墙、专线防火墙、上网行为管理为同一品牌。				
6	专线防火墙	AF-2000-FH2250B-F5	<p>1、网络层吞吐量 35Gbps，应用层吞吐量 20Gbps， 并发连接数 410 万，每秒新建连接≥18 万，电源：冗余电源，网络接口数：千兆电口 16 个，万兆光口 6 个， 配置 2 块万兆多模-850-300m-双纤。含 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测，提供三年 硬件质保及软件升级和 WEB 应用防护识别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL&应用识别库更新服务。</p> <p>2、支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>3、支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、 聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>4、支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀。</p> <p>5、支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的 运维与管理。</p> <p>6、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息。</p> <p>7、支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面。</p> <p>8、支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP。</p>	深信服/深圳	2 台	104250	208500

			<p>9、支持与本院现有态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。</p> <p>10、支持与本院现有服务器杀毒安全软件联动管理，在防火墙产品完成终端安全策略设置和服务器杀毒软件的统一管理，支持检测到某主机有僵尸蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离。</p>				
7	专线防火墙	AF-2000-FH2130B-F5	<p>1、网络层吞吐量 20Gbps，应用层吞吐量 9Gbps，并发连接数 200 万，每秒新建连接数 9 万，网络接口数：千兆电口 8 个，万兆光口 2 个。含 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测，提供三年硬件质保及软件升级和 WEB 应用防护识别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL& 应用识别库更新服务。</p> <p>2、支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>3、支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀。</p> <p>4、支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>5、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息。</p> <p>6、支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面。</p> <p>7、支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐</p>	深信服/深圳	2 台	63400	126800

			<p>获取黑客指纹信息，并自动封锁高危IP。</p> <p>8、支持与本院现有态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。</p> <p>9、支持与本院现有服务器杀毒安全软件联动管理，在防火墙产品完成终端安全策略设置和服务器杀毒软件的统一管理，支持检测到某主机有僵尸蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离。</p>					
8	网闸（核心产品）	SIS-3000-Z4500	<p>1、吞吐量(网络层流量)1200Mbps，最大并发连接数20万，2U设备，内网接口：6个千兆电口，6个千兆光口插槽，2个万兆光口插槽，一个扩展槽；外网接口：6个千兆电口，6个千兆光口插槽，2个万兆光口插槽，一个扩展槽；提供三年硬件质保、软件升级和安全规则库更新服务。</p> <p>2、具备文件交换、FTP访问、数据库传输、邮件传输、安全浏览、安全传输、消息模块等功能。</p> <p>3、内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以随时切换到B系统；且支持系统(包括配置)备份。</p> <p>4、支持IPv4/IPv6双栈网络环境，能够在IPv4/IPv6双栈网络环境下正常工作。</p> <p>5、文件同步支持格式特征过滤，并能提供文件类型判断工具以帮助用户识别不常见文件类型，判断工具支持的特征是可扩展的。</p> <p>6、支持Oracle、SQLServer、Sybase、Db2、MySQL、MongoDB、达梦、人大金仓、Gbase、神通、博阳等数据库同步；支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持。</p> <p>7、内/外网主机系统分别具有独立管理</p>	网御/北京	1台	127160	127160	

			<p>接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网 唯一管理接口完成全部管理等。</p> <p>8、支持用户身份认证，可对用户的客户端版本和进程进行检查，实现准入控制。</p> <p>9、为保持我院整体安全建设防护效果，要求网闸须与本项目防火墙异构。</p>				
9	WAF（核心产品）	Leadsec-6000WAF-800-M	<p>1、网络层 4Gbps，HTTP 应用层 220Mbps，HTTP 新建连接数 20000，HTTP 并发连接数 1000000，接口 6 千兆 电口。</p> <p>2、提供三年规则库升级，三年硬件质保、软件升级。</p> <p>3、支持旁路、透明、代理模式部署，支持基于 HTTP 协议的过滤功能、WEB 应用防护功能、WEB 攻击防护功 能、逃避检测防护功能、自定义错误页面功能，并支持规则库管理、报警、白名单、统计等功能。</p> <p>4、为保证产品对于 web 攻击检测的先进性和可靠性，系统应采用双引擎的检测机制，包括算法引擎和事件 引擎。</p> <p>5、具备 Web 恶意扫描防护的检测与防御能力。</p> <p>6、具备蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断，防止渗透网站。</p> <p>7、具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。</p> <p>8、具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置。</p> <p>9、具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对 Web 网站造成影响。</p> <p>10、为保持我院整体安全建设防护效果，WAF 与本项目防火墙异构。</p> <p>11、具备 CSRF 防护及自学习功能，能够有效防止 CSRF 攻击及通过自学习可减少 CSRF 配置，提供具备 CNAS、MA 标识的第三方机构出具的检测报告关键页复印件并加盖原厂商公章。</p> <p>12、为简化运维管理，要求 WAF 和网</p>	网御/北京	1 台	56420	56420

			同为同一品牌。				
10	上网行为管理	AC-1000-SK1200-1K	<p>1、网络层吞吐量 3G,带宽性能 200M,支持用户数 500, 最大并发连接数 12 万, 每秒新建连接数 2400, 网络 接口: 千兆电口 4 个, 提供三年硬件质保、软件升级和 URL 规则库更新服务。</p> <p>2、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。</p> <p>3、支持对网络接入的终端进行可视化 管理, 展示终端详细信息、合规状态等, 支持查看终端类型, 以及终端详细信息 (厂商, 系统, 端口等)。</p> <p>4、支持超过 9000 种以上应用规则数、支持超过 6000 种以上的应用; 支持根据标签选择应用, 并支持给每个应用自定义标签; 支持根据标签选择一类应用做控制。</p> <p>5、支持通过抑制 P2P 的下行丢包, 来减缓 P2P 的下行流量, 从而解决网络出口在做流控后仍然压力较大的问题。</p> <p>6、基于“流量”、“流速”、“时长”设置配额, 当配额耗尽后, 将用户加入到指定的流控黑名单 惩罚通道中; 用户指定应用上网流速超过预设阈值后, 网关自动提醒该用户。</p> <p>7、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; 空闲值可自定义。</p> <p>8、支持根据 IP、端口、协议等自定义应用规则; 支持根据端口设定用户不允许访问的目标 IP 组提供的服务; 支持根据不同的应用类型或具体的某种应用设置允许或拒绝。</p> <p>9、支持与本项目中三地接入防火墙-洪江区实现认证联动, 同时部署产品后, 可以实现认证同步机制, 实现 单点登录。</p> <p>10、为保障三院数据融合安全支持与总</p>	深信服/深圳	1 台	39500	39500

			院安全态势感知产品实现联动，实现资产信息上报。					
11	汇聚交换机	RS6300-26Q-EI-24X	<p>1、24 个千兆光口，2 个 40GEQSFP+光口，交换容量 2.56Tbps/23.04Tbps，包转发率 720Mpps/1260Mpps，配置 1 根堆叠线缆 SFP-10G-AOC-3M、4 个万兆多模光模块，提供 3 年的产品质保及软件升级服务。</p> <p>2、支持终端识别、终端准入、安全防护及安全画像可视。</p> <p>3、支持 LACP；支持手工聚合。</p> <p>4、支持对端口接收报文的速率和发送报文的速率进行限制。</p> <p>5、支持基于端口或堆叠口的 ACL 策略、基于源目 IP/MAC 地址的 ACL 策略、基于协议的 ACL 策略、基于时间的 ACL 策略。</p> <p>6、支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面。</p> <p>7、支持 Qos 特性，通过多种调度模式（例如：轮询模式、严格优先模式等）实现流量基于报文或端口的优先级。</p> <p>8、支持 DHCP Snooping，可将交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文。</p> <p>9、支持 STP、RSTP、MSTP 防环协议。</p> <p>10、支持 LACP；支持手工聚合。</p>	信锐/深圳	2 台	29400	58800	
12	核心交换机（核心产品）	RS3300-52T-4F	<p>1、48 个千兆电口，4 个千兆光口，交换容量 432Gbps/4.32Tbps，包转发率 132Mpps/166Mpps，提供 3 年的产品质保及软件升级服务。</p> <p>2、支持终端识别、终端准入、安全防护及安全画像可视。</p> <p>3、支持 LACP；支持手工聚合。</p> <p>4、支持对端口接收报文的速率和发送报文的速率进行限制。</p> <p>5、支持基于端口或堆叠口的 ACL 策略、基于源目 IP/MAC 地址的 ACL 策略、基于协议的 ACL 策略、基于时间的 ACL 策略。</p> <p>6、支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备</p>	信锐/深圳	2 台	4300	8600	

			有独立的控制平面。 7、支持 Qos 特性，通过多种调度模式（例如：轮询模式、严格优先模式等）实现流量基于报文或端口的优先级。 8、支持 DHCP Snooping，可将交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文。 9、支持 STP、RSTP、MSTP 防环协议。 10、支持 LACP；支持手工聚合。					
			合计				1538880.00	

2. 合同金额

(1) 合同金额小写：1538880.00

大写：壹佰伍拾叁万捌仟捌佰捌拾圆整

(2) 具体标的见附件。

(3) 合同定价方式：☒固定总价 ☐固定单价 ☐成本补偿 ☐绩效激励

(4) 付款方式（按项目实际勾选填写）：

☐全额付款：_____

☐预付款：_____

☒分期付款：设备均到医院进行安装并收到乙方合格发票后支付合同金额的 30%，设备验收合格并收到乙方合格发票后支付合同金额的 60%，设备验收合格后一年支付合同金额的 10%。

☐成本补偿：_____

☐绩效激励：_____

3. 双方的权利和义务：

(1) 乙方必须提供产品的有效证件资料，必须提供设备合格证，所有设备上均应有中文标识、生产日期等内容。

(2) 乙方负责为甲方免费调试安装至设备正常运转。

(3) 乙方负责安排生产厂家工作人员免费培训甲方的操作及维护人员。

(4) 乙方对产品提供（叁）年期硬件保修（设备保修期内，产品如发生故障或损坏由乙方负责免费维修。），保修期自怀化市第二人民医院验收报告单签字之日起计算。（叁）年期同等功能软件的免费升级服务（自设备上线交付之日起）。

(5)产品发生故障时，乙方的故障响应时间为2小时，维修到位时间为48小时。如产品故障在检修(48)个小时后未能排除故障进行修复，乙方应在(48)小时内免费提供不低于故障产品规格型号档次的备用产品供甲方使用，直至产品故障维修完毕。所有产品保修方式均为乙方上门保修，乙方派员至产品使用现场维修产生的一切费用均由乙方承担。服务期期满后，甲方需要乙方继续提供技术服务的，双方按照市场价格签订软硬件服务合同。

(6)乙方开出的发票必须真实合法有效，如开出虚假发票所造成的一切后果由乙方负责。

(7)甲、乙双方工作人员不允许有任何与购销相关的个人经济来往行为，坚决杜绝有商业贿赂行为发生，否则产生的任何后果及法律责任由相关人员承担，并取消乙方供货资格。

(8)甲方在使用过程中，应按照生产厂家所提供的操作说明书进行操作，如出现非属该设备品质的差错和医疗事故，乙方概不负责。甲方在使用过程中，亦不得擅自拆机或用仿制品代替原部件，否则一切后果自负。

4. 合同履行

(1) 签订合同后 30天内。

(2) 地点：怀化市第二人民医院鹤城院区信息中心机房。

(3) 履约担保：不要求提供。

(4) 质量保证金：不要求提供。

5. 合同验收

(1) 验收主体：怀化市第二人民医院。

(2) 验收方式：甲方组织验收。

(3) 验收标准：符合国家、行业、厂家标准。。

6. 组成合同的文件

本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释：

(1) 在采购或合同履行过程中乙方作出的承诺以及双方协商达成的变更或补充协议

(2) 本合同协议书

(3) 中标通知书

(4) 投标文件

(5) 政府采购合同专用条款

第二节 政府采购合同通用条款

1. 定义

1.1 合同当事人

(1) 采购人（以下称甲方）是指使用财政性资金，通过政府采购方式向供应商购买货物、服务的国家机关、事业单位、团体组织。本次采购的甲方名称、地址见【政府采购合同专用条款】。

(2) 供应商（以下称乙方）是指参加政府采购活动而取得中标结果，并向采购人提供货物、服务的法人、其他组织或者自然人。

1.2 本合同下列术语应解释为：

(1) “合同”系指甲乙双方签署的、政府采购合同协议书中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

(2) “合同价”系指根据本合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价款。

(3) “货物”系指乙方根据本合同规定须向甲方提供的各种形态和种类的物品，包括原材料、设备、产品（包括软件）及相关的其备品备件、工具、手册及其它技术资料 and 材料。

(4) “服务”系指根据合同规定，乙方应提供的技术、管理和其它服务，包括但不限于：管理和质量保证、运输、保险、检验、现场准备、安装、集成、调试、培训、维修、技术支持等以及合同中规定乙方应承担的其它义务。

(5) “合同条款”系指本合同及其附件、补充文件约定的全部条款。

(6) “项目现场”系指本合同项下货物安装、运行的现场，其名称见【政府采购合同专用条款】。

2. 合同的适用范围

2.1 本合同条款适用于没有被本合同其他部分的条款所取代的范围。

2.2 合同内容根据招标文件、投标文件而确定。

3. 合同标的及金额

3.1 合同标的及金额应与中标结果一致。

4. 合同价款

4.1 具体合同价款见本合同第 3.1 条。乙方为履行本合同而发生的所有费用均应包含在合同价款中，甲方不再另行支付其它任何费用。

5. 履行合同的时间、地点和方式

5.1 乙方应当在甲方确定的时间、指定的地点履行合同，具体的交货时间、地点和方式见【政府采购合同专用条款】。

5.2 乙方提供服务的应当在甲方指定的时间和地点完成服务项目。

6. 货物的验收

6.1 甲方在收到乙方交付的货物后应当及时组织验收。

6.2 货物的表面瑕疵，甲方应在验收时当面提出；对质量问题有异议的应在安装调试后十个工作日内提出。

6.3 在验收过程中发现数量不足或有质量、技术等问题，乙方应负责按照甲方的要求采取补足、更换或退货等处理措施，并承担由此发生的一切费用和损失。

6.4 甲方在乙方按合同规定交货或安装、调试后，无正当理由而拖延接收、验收或拒绝接收、验收的，应承担因此给乙方造成的直接损失。

6.5 甲方对货物进行检查验收合格后，应当收取发票并在《交货验收单》上签署验收意见及加盖单位印章。

6.6 大型或者复杂的货物采购项目，甲方可以邀请国家认可的质量检测机构参加验收工作，并由其出具验收报告单。

6.7 乙方提供的进口产品，乙方应出示中华人民共和国进出口商品检验部门出具的检验证书（招标文件第五章采购需求另有约定的除外）。

7. 货物包装要求

7.1 乙方所出售的全部货物均应按标准保护措施进行包装，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸等要求，以确保货物安全无损地运抵指定现场。由于包装防护措施不妥而引起的损坏、丢失由乙方负责。

7.2 每一个包装箱内应附一份详细装箱单、质量证书和保修保养证书。

8. 运输和保险

8.1 乙方负责办理将货物运抵本合同第 5.1 条规定的交货地点的一切运输事项，相关费用应包括在合同总价中。

8.2 乙方应向保险公司投保以甲方为受益人的发运合同货物发票金额的 110% 运输一切险。

9. 质量标准和保证

9.1 质量标准

(1) 本合同下交付的货物应符合招标文件第四章“技术规格、参数与要求”所述的标准。如果没有提及适用标准，则应符合中华人民共和国有关机构发布的最新版本的标准。

(2) 采用中华人民共和国法定计量单位。

(3) 乙方所出售的货物还应符合国家有关安全、环保、卫生之规定。

9.2 保证

(1) 乙方应保证所供货物是全新的、未使用过的，并完全符合合同规定的质量、规格和性能的要求。乙方应保证其货物在正确安装、正常使用和保养条件下，在其使用寿命期内应具有满意的性能，或者没有因乙方的行为或疏忽而产生的缺陷。在货物最终交付验收后不少于【政府采购合同专用条款】规定或乙方承诺（两者以较长的为准）的质量保证期内，本保证保持有效。

(2) 在质量保证期内所发现的缺陷，甲方应尽快以书面形式通知乙方。

(3) 乙方收到通知后应在【政府采购合同专用条款】规定的响应时间内以合理的速度免费维修或更换有缺陷的货物或部件。

(4) 在质量保证期内，如果货物的质量或规格与合同不符，或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第15.1条规定以书面形式向乙方提出补救措施或索赔。

(5) 乙方在约定的时间内未能弥补缺陷，甲方可采用必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同规定对乙方行使的其他权利不受影响。

10. 权利瑕疵担保

10.1 乙方保证对其出售的货物享有合法的权利。

10.2 乙方保证在其出售的货物上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

10.3 如甲方使用该货物构成上述侵权的，则由乙方承担全部责任。

11. 知识产权保护

11.1 乙方对其所销售的货物应当享有知识产权或经权利人合法授权，保证没有侵犯任何第三人的知识产权和商业秘密等权利。

11.2 甲方使用乙方提供的货物对第三人构成侵权的,应当由乙方承担全部法律责任,给甲方造成损害的,乙方应当承担赔偿责任。

11.3 甲方委托乙方开发的产品,甲方享有知识产权,未经甲方许可不得转让任何第三人。

12. 保密义务

12.1 甲、乙双方在采购和履行合同过程中所获悉的对方属于保密的内容,双方均有保密义务。

13. 合同价款支付

13.1 验收合格后,乙方出具正规发票给甲方,凭甲方开具的《政府采购合同验收报告单》办理合同价款结算手续。

13.2 合同价款构成中应当由财政支付的部分,甲方应当在货物验收合格后的十五个工作日内向国库管理部门申请支付,经国库管理部门审核后直接支付给乙方。

13.3 合同价款构成中应当由甲方自行支付的部分,甲方应当在货物验收合格后十五个工作日内支付。

13.4 支付合同价款时,一律不向乙方以外的任何第三方办理付款手续。开户行和账号以签订的政府采购合同为准,如果乙方要求变更,则乙方必须提供加盖了财务专用章、法定代表人签字的证明文件,报经甲方审查同意。

13.5 合同价款支付方式和条件在【政府采购合同专用条款】中另有规定。

14. 乙方应提供的服务

14.1 乙方应向甲方提交所提供货物的技术文件,包括相应的中文技术文件,如:产品目录、图纸、操作手册、使用说明、维护手册或服务指南。这些文件应包装好随同货物一起发运。

14.2 乙方还应提供下列服务:

- (1) 货物的现场移动、安装、调试、启动监督及技术支持;
- (2) 提供货物组装和维修所需的专用工具和辅助材料;
- (3) 在合同各方商定的一定期限内对所有的货物实施运行监督、维修,但前提条件是该服务并不能免除乙方在质量保证期内所承担的义务;
- (4) 在制造商或项目现场就货物的安装、启动、运营、维护对甲方操作人员进行培训;
- (5) 【政府采购合同专用条款】规定由乙方提供的其他服务。

14.3 乙方提供的服务的费用应包含在合同价款中,甲方不再另行支付。

15. 违约责任

15.1 质量瑕疵的补救措施和索赔

(1) 如果乙方提供的产品不符合质量标准或存在产品质量缺陷,而甲方在合同条款第9条或合同的其他条款规定的检验、安装、调试、验收和质量保证期内,根据法定质量检测部门出具的检验证书向乙方提出了索赔,乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜:

①乙方同意退货并将货款退还给甲方,由此发生的一切费用和损失由乙方承担。

②根据货物的质量状况以及甲方所遭受的损失,经过甲乙双方商定降低货物的价格。

③乙方应在接到甲方通知后七日内负责采用符合合同规定的规格、质量和性能要求的新零件、部件和设备来更换有缺陷的部分或修补缺陷部分,其费用由乙方负担。同时,乙方应在约定的质量保证期基础上相应延长修补和更换件的质量保证期。

(2) 如果在甲方发出索赔通知后十日内乙方未作答复,上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十日内或甲方同意延长的期限内,按照上述规定的任何一种方法采取补救措施,甲方有权从应付货款中扣除索赔金额或者没收质量保证金,如不足以弥补甲方损失的,甲方有权进一步要求乙方赔偿。

15.2 迟延交货的违约责任

(1) 乙方应按照本合同规定的时间、地点交货和提供服务。在履行合同过程中,如果乙方遇到可能妨碍按时交货和提供服务的情形时,应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。甲方在收到乙方通知后,应尽快对情况进行评价,并确定是否同意迟延交货时间或延期提供服务。

(2) 除本合同第20条规定情况外,如果乙方没有按照合同规定的时间交货和提供服务,甲方有权从货款中扣除误期赔偿费而不影响合同项下的其他补救方法,赔偿费按每周(一周按七天计算,不足七日按一周计算)赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五(0.5%)计收,直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五(5%)。一旦达到误期赔偿的最高限额,甲方可以终止合同。

(3) 如果乙方迟延交货,甲方有权终止全部或部分合同,并依其认为适当的条件和方法购买与未交货物类似的货物,乙方应对购买类似货物所超出的那部分费用负责。但是,乙方应继续执行合同中未终止的部分。

16. 合同的变更

16.1 在合同履行过程中,甲、乙双方可就合同履行的时间、地点和方式等协商进行变更。协商一致后,双方应签订书面的补充协议。

16.2 在不改变合同其他条款的前提下,甲方有权在合同价款百分之十的范围内追加与合同标的相同的货物或服务,并就此与乙方签订补充合同,乙方不得拒绝。

16.3 除双方签署书面协议,并成为合同不可分割的一部分外,本合同条件不得有任何变更。

17. 合同中止与终止

17.1 合同的中止

(1) 合同在履行过程中,因采购计划调整,甲方可以要求中止履行,待计划确定后继续履行;

(2) 合同履行过程中因供应商就采购过程或结果提起投诉的,甲方认为有必要或财政部门责令中止的,应当中止合同的履行。

17.2 合同的终止

(1) 合同因有效期限届满而终止;

(2) 乙方未能依照本合同约定条件履行合同,已构成根本性违约的,甲方有权终止本合同,并追究乙方的违约责任。

(3) 如果乙方丧失履约能力或被宣告破产,甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。

(4) 如果乙方在履行合同过程中有不正当竞争行为,甲方有权解除合同,并按《中华人民共和国反不正当竞争法》规定由有关部门追究其法律责任。

(5) 如果合同的履行将损害国家利益或社会公共利益,甲方有权终止合同的履行,给乙方造成损失的予以相应补偿。

18. 合同转让和分包

18.1 乙方不得以任何形式将合同转包。

18.2 乙方未在投标文件中说明,不得将合同的非主体、非关键性工作分包给他人。

19. 不可抗力

19.1 不可抗力是指合同双方不可预见、不可避免、不可克服的自然灾害和社会事件。

19.2 任何一方对由于不可抗力造成的部分或全部不能履行合同不承担违约责任。但迟延履行后发生不可抗力的,不能免除责任。

19.3 遇有不可抗力的一方,应在三日内将事件的情况以书面形式通知另一方,并在事件发生后十日内,向另一方提交合同不能履行或部分不能履行或需要延期履行理由的报告。

20. 争议解决的方法

20.1 合同各方应通过友好协商，解决在执行合同过程中所发生的或与合同有关的一切争端。如从协商开始后十日内仍不能解决，可以向财政部门提请调解。

20.2 调解不成可以向甲方所在地人民法院提起诉讼。

20.3 如仲裁或诉讼事项不影响合同其它部分的履行，则在仲裁或诉讼期间，除正在进行仲裁或诉讼的部分外，合同的其它部分应继续执行。

21. 法律适用

21.1 本合同适用中华人民共和国现行法律、行政法规和规章，如合同条款与法律、行政法规和规章不一致的，按照法律、行政法规和规章修改本合同。

22. 通知

22.1 本合同一方给另一方的通知均应采用书面形式，传真或快递送到本合同中规定的对方的地址和办理签收手续，

22.2 通知以送到之日或通知书中规定的生效之日起生效，两者中以较迟之日为准。

23. 合同未尽事项

23.1 合同未尽事项见【政府采购合同专用条款】，双方协商一致后签订书面补充协议。

24. 合同生效

24.1 本合同在合同双方签字盖章后生效。

第三节 政府采购合同专用条款

本章第二节 第 1.1 款	甲方名称、地址	名称：怀化市第二人民医院 地址：怀化市城东新区芦林路
本章第二节 第 1.2 (6) 项	项目现场	怀化市第二人民医院
本章第二节 第 5.1 款	履行合同的时间、 地点及方式	时间：30 天 地点：采购人指定地点 方式：按合同约定
本章第二节 第 9.2 (1) 项	质量保证期	按合同约定
本章第二节 第 9.2 (3) 项	响应时间	按第五章采购需求响应。
本章第二节 第 13.5 款	合同价款支付方 式和条件	按合同约定
本章第二节 第 14.2 (6) 项	乙方提供的其他 服务	按第五章采购需求。
本章第二节 第 23.1 款	合同未尽事项	协商解决