合同编号：YHT-2026-88

# 陕西西咸新区人民法院信息网络设备购置项目

# 施

# 工

# 合

# 同

发包人：陕西西咸新区人民法院
承包人：陕西亿弘通电子科技有限公司

签订日期：2026年11月9日

# 第一部分 合同协议书

甲方（发包人）：陕西西咸新区人民法院

乙方（承包人）：陕西亿弘通电子科技有限公司

依据《中华人民共和国民法典》《建设工程质量管理条例》《安全防范工程技术标准》（GB50348-2018）《智能建筑工程质量验收规范》（GB50339-2013）等相关法律法规及行业标准，甲乙双方本着平等自愿、公平诚信、互利共赢的原则，就上和里小区智能化系统的设备采购、运输、安装、调试、培训、验收及售后质保等相关事宜，经友好协商，达成如下协议，以资共同信守。

## 一、工程概况

1. 工程名称：信息网络设备购置项目

2. 工程地点：陕西西咸新区人民法院

3. 工程内容：乙方负责本院网络系统漏洞扫描、Web 应用防火墙、APT 攻击预警平台、入侵防御系统、网络安全审计系统、网络准入系统、统一管理平台、安全接入网关系统的设备采购、运输、装卸、布线、安装、调试、系统联调、人员培训、竣工验收及售后质保等全流程服务，所有主设备选用招标文件规定的品牌，并确保系统稳定、安全、高效运行。

4. 承包模式：乙方采用“包工、包料、包设备、包运输、包安装、包布线、包调试、包验收、包培训、包质保、包售后”的全包模式，合同总价为含税固定总价，无任何隐形增项费用。

5. 工期要求：本工程总工期为 45 日历天，自甲方出具书面开工通知且乙方收到预付款之日起计算，至工程全部竣工、调试合格并通过甲方及物业联合验收之日止。若因甲方场地条件不具备、土建施工交叉影响、甲方逾期付款或不可抗力等非乙方原因导致工期延误，工期相应顺延，乙方不承担违约责任。

## 二、合同总价款及支付方式

本工程含税总造价：￥608505.89 元（大写人民币：陆拾万捌仟伍佰零伍元捌角玖分）税率 9%普通发票，不含税造价：￥558262.28 元（大写人民币：伍拾伍万捌仟贰

佰陆拾贰元贰角捌分），税金：50243.61（大写人民币：伍万零贰佰肆拾叁元陆角壹分）。

1、该价款包含所有设备采购费、运输装卸费、辅材费、线缆桥架费、开槽修复费、人工安装费、系统调试费、平台对接费、检测验收费、图纸资料费、操作人员培训费、3 年免费质保、上门维修费、税金等相关费用，甲方无需另行支付其他任何费用。

2. 发票约定：乙方应向甲方开具合法有效的增值税普通发票，发票税率为 9%，发票抬头、内容等需符合甲方财务要求，甲方收到发票后按合同约定支付相应款项。

3. 付款方式：甲方通过银行转账方式将款项支付至乙方指定收款账户，乙方指定收款账户信息如下：

开户行：交通银行股份有限公司榆林支行

户名：陕西亿弘通电子科技有限公司

账号：612899991015003025272

4. 付款方式：①40%预付款；②竣工验收后，支付结算价款的 60%；

## 三、质量标准及设备要求

1. 设备质量标准：乙方所供设备均为全新原厂正品，符合国家及行业相关质量标准，具备产品合格证、3C 认证、检测报告等相关资质文件，数量等详见附件一《设备材料报价清单》。

2. 辅材质量标准：系统配套辅材（网线、电源线、桥架、管材、电源、机柜等）均采用国标合格产品，网线选用国标超六类非屏蔽双绞线，电源线选用 RVV 系列国标线缆，桥架采用镀锌防火桥架，管材采用 PVC/KBG 国标管材，确保辅材质量符合工程施工及使用要求。

3. 施工质量标准：乙方严格按照《安全防范工程技术标准》（GB50348-2018）、《智能建筑工程质量验收规范》（GB50339-2013）及本合同约定的施工方案进行施工，布线做到横平竖直、强弱电分离，隐蔽工程施工后及时拍照、录像留档，经甲方确认后方可进行后续施工，防雷接地、设备固定等施工环节符合行业规范，确保工程施工质量达标。

4. 系统功能标准：各子系统功能需满足本合同约定及甲方使用需求，实现互联互通、联动控制。具体功能要求如下：

| 序号 | 产品名称 | 技术参数与性能指标 | 备注 |
| --- | --- | --- | --- |
| 1 | 漏洞扫描 | 数量/单位：1/台　　核心产品<br>1.设备采用国产化 CPU、国产化操作系统，配置千兆电口≥8 个，支持扩展槽≥2 个，USB 接口≥2 个，配置冗余电源；<br>2.内存≥16GB，硬盘存储≥1T；<br>3.支持配置主机漏洞模板，内置漏洞库数量≥200000 种，可兼容 CVE、CNNVD、CNVD 等主流标准，同时支持自定义扫描漏洞库，漏洞库类型可基于操作系统、数据库、中间件等进行分类；<br>4.支持快速摸排资产、精准定位风险隐患，及时响应通报并推动整改，帮助用户进行资产梳理，评估风险影响，形成安全管理闭环；<br>5.支持旁路部署模式，支持分级部署与集中管理，IP 检测，无需改变网络架构，基于 WEB 进行管理；<br>6.支持系统安全配置核查功能，能够对主流操作系统、数据库、中间件、网络设备等安全配置项目进行检查；<br>7.可创建并下发资产盘点任务，检测任务可发现目标范围内在线的资产，可检测到在线资产的 IP 地址、 MAC 地址、操作系统、资产类型、设备厂商、设备型号、软件版本，并在报告中展示设备开放的高危端口；（提供该功能的佐证材料）<br>8.支持对高危漏洞的自动化验证功能，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现；<br>9.平台具备安全可视化监测界面，7×24h 监控资产状态及安全风险态势。可展示当前检测任务进度、最新漏洞情况、弱口令统计、高危端口统计、资产类型统计、资产风险分析以及模拟人工渗透等内容；<br>10.配置：域名扫描授权不少于 64 个，漏洞库升级服务授权 3 年，原厂质保 3 年。 | |

| | | | |
|---|---|---|---|
| 2 | Web应用防火墙 | 数量/单位：1/台<br>1.设备采用国产化CPU、国产化操作系统，具备千兆电口≥8个，千兆光口≥4个，支持扩展槽≥2个，配置冗余电源 ；<br>2. 整机吞吐≥6Gbps，HTTP吞吐≥800Mbps，最大并发连接数≥250万，每秒新建连接数≥1.6万；<br>3.支持透明模式、代理模式、网关模式和旁路模式，且模式之间切换不需要重启设备或者检测引擎，可多种模式共同运营；<br>4.支持通过虚拟化技术实现将一台物理设备虚拟成不少于100个虚拟WAF；并且可对每个虚拟WAF使用的资源进行限制，例如会话数、新建速率、吞吐量、CPU及内存使用率；（提供该功能的佐证材料）<br>5.支持流量自学习，可以自动学习IP、域名、端口等信息，将学习到的服务添加到防护策略；<br>6.支持基于全局设定头域字段名最大长度、头域字段值最大长度，以及是否禁止重复头域进行设定，防止头域异常数据导致的服务器问题；支持HOST、Referer、User-Agent、Range、Accept、Accept-Charset、Content-Length、Content-Encoding等正规化规则设定，有效避免特定头域字段值不符合RFC标准规范要求；<br>7.支持通过设定前置参数名、正则表达式、参数范围等匹配特定的主机名、URL，对容易被篡改或者篡改会产生重大风险的参数名的取值进行限定；<br>8.支持CSRF防护，通过设置HOST、URL、Referer、积极模式串等参数，对访问服务器的请求进行CSRF过滤和检测；<br>9.支持通过对经过设备的流量进行学习，学习并展示URL、参数、Cookie等信息，支持针对特定URL的请求频率、最大长度、参数个数、Cookie总长度等进行策略配置，支持对学习到的参数的类型、最大值、最小值进行限制，智能形成防护策略,；<br>10.配置：特征库升级服务授权3年，原厂质保3年。 | |

| | | | |
|---|---|---|---|
| 3 | APT攻击预警平台 | 数量/单位：1/台<br>1.设备采用国产化CPU、国产化操作系统，配置千兆电口≥4个，con口≥1个，支持扩展槽≥2个；CPU ≥8核，内存≥64GB，存储≥4T；配置冗余电源；<br>2.网络层吞吐≥2Gbps，应用层吞吐≥1Gbps；<br>3.支持对HTTP/FTP/SMB/SMTP/POP3/TFTP等类型协议流量中出现文件传输行为进行发现和还原；<br>4.支持自定义威胁情报，支持根据威胁类型、威胁名称、威胁等级、置信度、IP等自定义添加威胁情报；<br>5.支持告警事件分析，能够展示安全事件告警级别、攻击类型、影响主机、攻击状态、攻击IP、协议、攻击位置、目标位置情况；<br>6.支持跳转展示攻击详情，展示安全事件请求信息、响应信息、原始数据包信息，针对攻击事件提供详细解释说明，并提供相应的解决方案；<br>7.支持监测流量状态，基于时间维度记录并展示流入、流出流量情况，并记录流量的总流入流出情况。支持安全流量监测的开关控制；（提供该功能的佐证材料）<br>8.支持恶意文件沙箱分析功能，分析结果包括但不限于恶意文件名称、受感染主机、动态检测结果、传播次数、病毒类型、处理状态。支持跳转展示沙箱分析详情，展示文件的静态检测、动态检测、病毒检测结果；（提供该功能的佐证材料）<br>9.支持挖矿威胁专项分析能力，分析结果包括但不限于攻击名称、矿池IP地址、矿池位置、威胁情报、协议、告警时间，支持下载挖矿原始报文；<br>10.支持多种病毒检测引擎，集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于20000条；<br>11.支持边界完整性检测，可针对专网中的非法外联主机进行有效检测和定位，可检测出目标设备的违规外联行为；<br>12.配置：特征库升级服务授权3年，原厂质保3年。 | |

| | | | |
|---|---|---|---|
| 4 | 入侵防御系统 | 数量/单位：1/台<br>1.设备采用国产化 CPU、国产化操作系统，具备千兆电口≥8 个，千兆光口 4 个，支持扩展槽≥2 个，配置冗余电源；<br>2.整机网络层吞吐≥5Gbps，防攻击、防病毒吞吐量≥800Mbps，最大并发连接数≥300 万，每秒新建连接数≥2 万；<br>3.支持透明、在线、旁路三种部署模式；<br>4.支持隧道报文检测，可以识别并检测 VLAN，QINQ，MPLS，GRE，VXLAN，PPPOE 等常见协议封装的网络报文，增强复杂网络适应性；<br>5.内置 IPS 特征库，可针对 SQL 注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量不少于 9000 条；<br>6.支持对不同等级的攻击特征设置不同的动作（告警、阻断、阻断+源/目的/双向 TCP Reset），且可以设置例外特征 ID；<br>7.支持自定义 IPS 特征，可基于方向、父协议、字符串、正则表达式、源端口、目的端口等维度进行特征自定义，并可自行设置特征严重等级（告警、一般、严重、致命、废除）；<br>8.入侵防御检测支持自定义检测阈值来自动下发黑名单进行攻击阻断，黑名单生效时间可以自定义；<br>9.入侵防御日志支持聚合发送，聚合条件包括源 IP 聚合、目的 IP 聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器不少于 10 个；<br>10.支持收集流入目标网络内所有数据包，并对收集的数据包进行协议分析，用以拦截拒绝服务类攻击、木马类攻击、溢出类攻击入侵行为；<br>11.配置：特征库升级服务授权 3 年，原厂质保 3 年。 | |

| | | | |
|---|---|---|---|
| 5 | 网络安全审计系统 | 数量/单位：1/台<br>1.设备采用国产化 CPU、国产化操作系统，具备接口：千兆电口≥8 个，千兆光口≥4 个，支持扩展槽≥2 个；<br>2.网络层吞吐≥10Gbps，并发连接数≥180 万，新建连接数≥1.2 万；<br>3.支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理；<br>4.支持 NAT 功能，支持源 NAT、目的 NAT、一对一 NAT 的等功能；<br>5.支持会话监控功能，支持统计设备会话数、IPv4、IPv4 TCP、IPv4 UDP、IPv6、IPv6 TCP、IPv6 UDP 并发会话数等及趋势图信息；<br>6.支持诊断功能：支持设备页面抓包，报文回放。页面抓包支持 IP 地址、协议、接口、抓包方向、抓包时间、抓包数量等多种灵活的过滤条件，抓取需要的流量报文，支持基于接口回放报文；<br>7.URL 地址库≥1200 万，当地址库中不存在时支持自定义添加 URL 地址；<br>8.系统内设应用协议库，支持识别协议明细数量条目≥6000 条；<br>9.可基于用户、时间、VLAN 和协议等进行细粒度流量管理，可为核心业务动态预留资源，在出现网络资源不足时，优先保障核心业务的通畅运行；<br>10.配置：特征库升级服务授权 3 年，原厂质保 3 年。 | |
| 6 | 网络准入系统 | 数量/单位：1/台　　核心产品<br>1.CPU≥8 核、内存≥32G、存储空间≥8T，千兆电口≥4 个；满足国产化自主可控要求。<br>2.支持策略场景定义客户端在线、客户端离线等状态，可从以下维度：互联网状态、本地 IP 范围、终端在线情况、VPN 状态、网卡使用状态等定义。<br>3.支持准入控制与桌面管理、终端安全、软件管理、补丁管理、防病毒、终端检测与响应、数据交换、数据防泄密、文档加解密由同一管理平台、同一终端客户端原生提供，用户、终端、组织和策略对象只维护一次；不接受多套客户端或依靠第三方接口拼接。<br>4.提供轻量级面向对象脚本，实现复杂功能调用或是多种检查功能，作为辅助脚本执行定时、循环的机械化操作；（提供该功能的佐证材料）<br>5.本次授权至少 500 台终端准入控制许可（需不受操作系统限制的授权）； | |

| | | | |
|---|---|---|---|
| | | 6.支持客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除；客户端正常运行情况下安装目录隐藏；<br>7.支持客户端功能热更新、无需重启服务或设备；<br>8.支持客户端安全模式下运行，客户端策略依然生效；<br>9.支持 Windows、macOS、Linux 客户端、国产化统信 UOS/麒麟等操作系统；<br>10.支持 802.1X、Portal/WebAuth、MAB/设备指纹、端口镜像、策略路由等多种准入方式单独或混合部署，并能在一个管理后台统一查看准入结果。<br>11.支持终端修复向导，内置向导页面内容可编辑，同时也支持 URL 外链修复页面；<br>12.支持主流交换机在 802.1X 场景下直接下发 ACL 动态规则，无需在交换机预先逐端口或逐用户手工配置 ACL 模板，并支持策略变更后动态生效。<br>13.支持阻止非授权虚拟机接入网络的能力和功能；<br>14.支持对接入网络的终端进行发现和定位；<br>15.支持自动发现识别接入设备的类型，包括：PC 设备、网络设备、服务器、移动设备、IoT 设备等，终端操作系统：Windows、MAC、Liunx 等操作系统；<br>16.支持自动识别指定 AD 域、邮件服务器的 PC，自动准入放行并下发权限控制策略；<br>17.支持管理员以 web（网页）方式远程协助 window 或信创电脑，具备终端主动求助、授权发起协助、会话过程提示、键盘鼠标控制、文件双向传输、超时自动断连、协助提示语自定义等能力；支持按网络环境灵活配置中继节点、网段匹配及服务端口，实现远程运维访问控制、过程留痕、统一策略下发与安全审计管理。<br>18.支持对软件进行全网分发，软件静默安装，安装过程员工无感知；<br>19.支持闲时终端关机、注销、锁定、重启、睡眠、休眠、关闭显示器等操作；<br>20.支持对软件及 CPU、内存、显卡、硬盘、主板、网卡等资产变更进行监控审计，重点支持硬盘拆卸、更换审计。<br>21.支持通过 PING/TCP/HTTP 等方式检测终端是否与互联网或其他网络连接，并支持处置：断网/锁屏，直到事件恢复或由管理员恢复；<br>22.支持 USB、共享 WiFi、蓝牙、光盘、智能设备、串并口等外设管控；支持无线网卡与 WiFi 管控、Linux 和 macOS 外设控制、AirDrop 审计阻断，以及基于设备属性和外联检测的阻断处置。 | |

| | | | |
|---|---|---|---|
| | | 23.支持 Windows、macOS、Linux 及国产化统信 UOS、麒麟终端的统一合规检查，至少覆盖补丁、防病毒/EDR、弱口令、共享、进程、服务、端口、防火墙、屏保等内容，检查项按操作系统分别配置，并支持自定义检查项，不合规终端给出整改提示；支持软件、补丁、弱口令等一键修复能力，可通过客户端进行一键自动修复自动下载安装，无需用户手动下载安装。<br>24.将认证用户与终端硬件唯一标识、MAC 地址、接入交换机端口或接入控制点组合绑定，支持一人一机、一人多机及允许设备数量限制；绑定异常时不得直接沿用原权限；<br>25.支持手动快速逃生方式，可在系统后台一键切换至准入放行模式； | |
| 7 | 统一管理平台 | 数量/单位：1/套<br>1.现网设备管理：支持对安全设备进行集中管理，可通过访问控制策略的配置，实现大规模部署环境下的灵活、便捷的安全策略管理，阻止敏感信息外泄和非核心业务的滥用，确保网络的整体安全；<br>2.整网信息分析：全面集成日志采集器、数据库、日志分析、审计、报表等功能部件，可实现对整张网络进行全面的网络流量分析，自动关联安全事件，帮助管理员实时了解整网状况，发现潜在安全风险，保障网络安全；<br>3.部署管理：支持集中管理和分级管理两种模式。集中管理可以在统一管理平台上针对网络中所有设备进行统一的配置和安全事件管理；对于较大规模和分区域的网络环境，统一管理平台上还支持通过分级管理的方式进行总部和分部的统一管理；<br>4.远程管理：采用 B/S 架构，内建 HTTP 服务器，管理员可以在任意位置通过 HTTP 或 HTTPS 方式登录统一管理平台对网络进行监控和管理；<br>5.支持攻击事件分析，可以分析攻击事件趋势、事件分布、目的、来源、目的端口、协议、类型、级别、位置等多维度的事件快速分析统计，并支持直接导出相应的分析结果报表。<br>6.支持攻击态势概览展示，可展示攻击事件趋势、TOP 攻击事件、TOP 攻击目的端口、TOP 攻击目的、TOP 攻击源等信息。<br>7.支持综合事件监控，对设备的攻击防护、病毒防护进行综合统计，展示相应的事件数、阻断情况、攻击目的/源 IP 地址数、攻击目的端口数。<br>8.支持攻击事件明细展示，可通过设备 IP、攻击源 IP、攻击目的 IP、事件类型、协议、端口等条件筛选，展示内容包含时间、设备 IP、入接口、攻击源 IP/端口、源归属、攻击目的 IP/端口、目 | |

| | | | |
|---|---|---|---|
| | | 的归属、事件类型、事件、事件数等信息，同时支持查看攻击报文。<br>9.支持攻击报表导出，可以自定义报表，可选则整体安全分析（包含攻击趋势分析、高危风险分析、攻击类型分析、攻击事件分析、被攻击 IP、攻击源 IP），系统安全分析（被攻击 IP 分析、攻击来源 IP 分析），报表导出格式可以设置 PDF 或 DOC。<br>10.支持安全事件态势概览，展示攻击防护、病毒防护整体情况，包含总攻击事件数、阻断事件数、攻击源 IP 地址数、攻击目的 IP 地址数、事件种类等；支持 TOP 维度统计展示，包含 TOP 攻击事件、TOP 攻击目的 IP。<br>11.支持对攻击地址进行信息研判，可展示该地址流入 / 流出流量、应用流量信息，可呈现攻击 IP、攻击手段、攻击次数等相关信息。<br>12.巡检：支持对整网设备进行手动/定期巡检；支持自定义巡检规则，支持巡检规则的导入及导出；支持查看及下载巡检报告；<br>13.支持业务流量趋势报表的导出功能。添加报表导出任务后，系统可按照报表任务指定的周期和报表格式自动导出报表，并将报表发送至指定的收件人，同时支持手动导出报表；<br>14.配置：不少于 5 个设备授权。 | |
| 8 | 安全接入网关 | 数量/单位：1/台<br>1.千兆电口≥20 个，万兆光口≥4 个，支持可热插拔冗余双电源；满足国产化自主可控要求。<br>2.终端管理：<br>①支持对终端的批量修改、导入、导出、白名单、黑名单操作；<br>②支持集中展示在终端数量及状态、终端类型 Top 排名、接入绑定状态；支持展示终端描述、MAC、IP、接入绑定、终端群组、接入时间、离线时间等信息。<br>3.终端组管理：<br>①支持基于业务需求自定义终端群组，通过 VLAN 等策略实现实现终端策略随行；<br>②支持终端管理组织配置与设备管理组织配置同步，提升终端群组的分群组管理效率。<br>4.终端类型：<br>①支持自定义终端属性、终端类型，并可基于现网接入设备自动提取终端 OUI 指纹信息；<br>②支持联动现网扫描设备实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验。<br>5.终端查询： | |

| | | | | |
|---|---|---|---|---|
| | | ①支持根据终端 IP、终端 MAC、终端描述、终端类型、标记、接入绑定、终端状态、阻断情况、离线时长进行查询；<br>6 终端绑定：<br>①支持基于自定义终端、设备群组、全局进行终端绑定配置；<br>②支持设定 IP 地址、MAC 地址、接入位置三元素任意组合的绑定策略；<br>③支持对于自定义时长后未接入终端的自动解绑；<br>④支持自动删除自定义时长离线后终端的自动删除；<br>⑤支持阻断未绑定终端，仅允许已绑定终端接入<br>7.资源管理：<br>支持 IP 资源管理功能，可根据业务需要自定义添加所关注的子网网段，平台可直观展示内网 IP 资源利用情况<br>8.安全管理：<br>①支持防终端私接功能，可针对自定义终端类型一键下发阻断策略；<br>②支持对仿冒终端的识别判定及阻断<br>③支持自定义第三方设备 OUI 值形成库，配合网络设备对于其中终端可进行私接防护；<br>④支持阻断终端的所有报文，包括 ARP、DHCP 等报文；<br>⑤支持对 LAND、死亡之 Ping、IP 分片重叠、UDP Fraggle、WinNuke、ICMP Smurf、Tear Drop、逐跳选项、分片首部、伪首部等常见畸形包攻击进行检测防护，可根据网络需求自定义防护级别；<br>⑥支持基于用户设定新建速率、总会话数、TCP 会话数、UDP 会话数等阈值进行监控告警和阻断；<br>⑦支持对 TCP、ICMP、UDP、分片报文等协议下报文速率进行精细化阈值设置，可基于源 IP、目的 IP、syn/ack/fin/http 等类型报文速率进行自定义观察/限速/阻断操作<br>⑧支持对病毒感染主机的网络隔离功能，可在终端感染，病毒后能够识别并阻断病毒传播，同时不影响终端业务（例如文件共享业务）；<br>9.处置工作台：<br>①支持通过安全事件分布、终端安全事件 TOP 排行、安全事件趋势、安全阻断分析等维度展示整网安全概况；<br>②支持展示内网异常告警及阻断终端，并展示异常时间、异常原因及告警设备；<br>③支持入网审批功能，实现新入网终端的桌面化一键审批入网。<br>10.配置：特征库升级服务授权 3 年，原厂质保 3 年。 | |

| | | | |
|---|---|---|---|
| 9 | 实施安装调试 | 数量/单位：1/项<br>负责设备上架、网络设备设备调试等 | |

## 四、双方责任与义务

### （一）甲方责任与义务

1. 为乙方提供施工所需的场地、临时水电接驳点，协调小区内土建、装修、电梯、物业等各方，配合乙方完成交叉施工，确保乙方施工顺利进行。

2. 向乙方提供施工所需院区平面图纸、弱电井位置、机房位置、管线预埋预留等相关资料，指定专人作为现场对接人，及时确认施工方案、设备型号、工程变更等相关事宜。

3. 按合同约定按时支付工程款项，不得无故拖欠。若因甲方逾期付款导致工期延误或乙方损失，由甲方承担相应责任。

4. 组织设备到货验收、分阶段施工验收及整体竣工验收，及时签署相关验收文件。验收过程中发现问题的，及时书面通知乙方，配合乙方完成整改工作。

5. 工程竣工后，安排院区管理人员参加乙方组织的操作培训，配备专职操作人员，妥善保管乙方移交的竣工图纸、设备说明书、软件操作手册、账号密码等相关资料，规范操作使用智能化系统。

6. 负责协调院区及相关人员，配合乙方施工，避免因业主阻挠、干扰导致施工无法正常进行。

### （二）乙方责任与义务

1. 严格按照本合同约定及附件《设备材料报价清单》采购设备，确保主设备约定品牌的全新原厂正品，提供设备出厂合格证、3C 认证、检测报告、原厂质保承诺函等相关资质文件，甲方可随机核验设备真伪，若发现设备不符合约定，乙方需无条件更换，并承担相应违约责任。

2. 负责设备的运输、装卸工作，承担运输、装卸过程中的设备损坏、丢失等风险，确保设备安全、完好到场。设备到场后，及时通知甲方进行清点验收，签署《设备到货验收单》。

3. 负责工程现场的布线、设备安装、机房布置、防雷接地等施工工作，施工过程中遵守院区安全管理规定，文明施工，施工垃圾及时清理，对施工过程中造成的院区路面、墙面、绿化等损坏，负责免费修复，恢复原貌。

4. 负责所有子系统的单机调试、跨系统联调工作，确保系统运行稳定、功能达标，完成 72 小时不间断试运行，试运行合格后向甲方提交竣工验收申请及全套竣工资料。

5. 免费为甲方及管理人员提供不少于 1 次系统操作培训，确保操作人员能够熟练掌握系统使用方法。

6. 严格遵守安全生产相关规定，承担施工期间的人员安全、设备安全及第三方安全责任，施工过程中发生的任何安全事故、人员伤亡、财产损失及第三方索赔，均由乙方全部承担，与甲方无关。

7. 履行质保义务，质保期内提供免费上门维修、设备更换等服务，接到故障报修后，工作时间 4 小时内到达现场，夜间、节假日紧急故障 8 小时内到达现场，无法现场修复的，48 小时内提供备用设备替换，确保系统正常运行。

8. 对本合同内容、院区安防布局、设备点位、业主信息等相关资料严格保密，不得向任何第三方泄露，否则承担相应法律责任及经济赔偿责任。

# 第二部分 专用合同条款

## 五、设备供货与到货验收

1. 乙方应提前 3 个工作日书面通知甲方设备到货时间、地点，甲乙双方共同到场进行开箱清点验收，核对设备品牌、型号、参数、数量、外观完好度等，验收合格后签署《设备到货验收单》，设备所有权自验收合格之日起转移至甲方，验收合格前的设备风险由乙方承担。

2. 若验收过程中发现设备品牌、型号、参数与合同约定不符，或设备存在破损、故障、假冒伪劣等情况，乙方需在 3 个工作日内无条件更换为符合约定的全新正品设备，承担由此产生的运输费、装卸费等所有费用，若因此导致工期延误，乙方承担相应违约责任。

3. 设备到场后，由乙方负责设备的保管工作，直至工程竣工验收合格，期间发生设备丢失、损坏等情况，由乙方承担全部责任，负责免费更换或维修。

4.合同签署后乙方开始备货，甲方预付款支付后乙方开始进场施工，本工程总工期为 45 日历天，自甲方出具书面开工通知且乙方收到预付款之日起计算，至工程全部竣工、调试合格并通过甲方及物业联合验收之日止。

## 六、工程变更与增项

1. 本工程施工过程中，甲方如需对系统点位、设备型号、功能要求等进行变更，或增加工程量，需向乙方出具书面《工程变更签证单》，明确变更内容、变更原因、变更价款及工期调整等事宜，经甲乙双方签字盖章确认后，方可作为工程施工及结算的依据。

2. 乙方不得擅自变更工程内容、调整设备型号或增加工程量，若因乙方擅自变更导致工程质量不达标、工期延误或甲方损失，由乙方全部承担责任，甲方不予结算相关费用。

3. 工程变更价款的计算方式：按附件《供货清单及明细》中约定的单价及实际变更工程量进行核算，无对应单价的，由双方协商确定。

## 七、验收流程与标准

1. 单机调试验收：乙方完成每个子系统的安装及单机调试后，自行自检合格，向甲方提交单机调试验收申请，甲方在收到申请后 3 个工作日内组织现场查验，查验合格后签署《单机调试验收单》，不合格的，乙方需限期整改，整改合格后重新申请验收。

2. 72 小时试运行：所有子系统单机调试验收合格后，乙方组织系统联调，完成后进行 72 小时不间断试运行，试运行期间系统无死机、断连、频繁误报、识别失效等故障，视为试运行合格；若试运行不合格，乙方需排查故障、限期整改，整改完成后重新进行试运行，直至合格。

3. 整体竣工验收：试运行合格后，乙方向甲方提交竣工验收申请，并移交全套竣工资料（包括竣工 CAD 图纸、设备材料清单、设备说明书、软件操作手册、账号密码、产品合格证、检测报告、调试记录、验收记录等），甲方在收到申请及资料后 3 个工作日内，组织甲方、乙方联合验收，验收合格后签署《竣工验收合格单》，质保期自签署之日起计算；验收不合格的，乙方需在甲方指定的期限内完成整改，整改费用由乙方承担，若逾期未整改，甲方有权委托第三方进行整改，整改费用从工程款中扣除，同时乙方承担相应违约责任。

4. 验收标准：严格按照本合同约定的质量标准、系统功能标准及国家、行业相关规范执行。

## 八、质保与售后服务

1. 本工程整体质保期为 3 年，自竣工验收合格并签署《竣工验收合格单》之日起计算；所有主设备同步享受品牌原厂官方质保，原厂质保期超出本合同质保期的，按原厂质保期执行。

2. 质保范围：质保期内，因设备本身质量问题、施工工艺问题、系统软件问题导致的故障，乙方提供免费上门维修、设备更换、软件调试等服务；因甲方人为损坏、不可抗力、第三方破坏、违规操作等原因导致的故障，不在免费质保范围内，乙方可提供有偿维修服务，仅收取材料成本费，不收取上门工时费。

3. 售后响应要求：乙方建立完善的售后服务体系，设立 24 小时售后服务热线：赵彦龙：15529736888，接到甲方或物业的故障报修后，工作时间（9:00-18:00）4 小时内到达现场，夜间、节假日紧急故障（如系统瘫痪、大面积报警等）8 小时内到达现场，

对故障进行排查、维修；若故障无法现场修复，乙方需在 48 小时内提供同型号、同规格的备用设备替换，确保系统正常运行，待故障设备修复后，再换回备用设备。

4. 质保期满后，乙方可向甲方提供终身优惠维保服务，维保费用由双方另行协商签订维保协议，乙方承诺维保期间收取的材料成本费不高于市场同期价格，且免费提供软件远程调试、平台账号维护、固件升级等服务。

5. 乙方需在质保期内定期对系统进行巡检，每季度至少巡检 1 次，及时排查潜在故障，做好巡检记录，反馈给甲方及物业，确保系统长期稳定运行。

## 九、违约责任

1. 甲方违约责任：甲方未按本合同约定按时支付工程款项，每逾期一日，按应付未付款金额的 0.05%向乙方支付违约金；逾期超过 30 日的，乙方有权暂停施工，工期相应顺延，同时甲方需承担乙方因此产生的停工损失、设备保管费等相关费用；若甲方逾期付款超过 60 日，乙方有权单方面解除合同，甲方需支付乙方已完成工程量的全部款项，并按合同总价款的 10%向乙方支付违约金。

2. 乙方违约责任：

（1）乙方未按合同约定的工期完成工程施工及验收，每逾期一日，按合同总价款的 0.1%向甲方支付违约金，累计违约金不超过合同总价款的 10%；逾期超过 30 日的，甲方有权单方面解除合同，乙方需退还甲方已支付的全部款项，并按合同总价款的 10%向甲方支付违约金，同时承担甲方因此产生的损失。

（2）乙方提供的设备为假冒伪劣、翻新、贴牌或与合同约定品牌、型号不符的，视为根本性违约，甲方有权单方面解除合同，乙方需全额退还甲方已支付的所有款项，额外按合同总价款的 20%向甲方支付违约金，并在 3 个工作日内拆除全部不合格设备，恢复现场原貌，承担由此产生的所有费用。

（3）工程施工质量、系统功能不符合本合同约定及相关规范标准，乙方需限期整改，整改费用由乙方承担，若整改后仍不合格，甲方有权委托第三方施工，费用从工程款中扣除，同时乙方按合同总价款的 10%向甲方支付违约金。

（4）乙方未履行质保义务，接到故障报修后未按约定时间到场，或未按约定提供维修、更换服务，每逾期一日，按合同总价款的 0.05%向甲方支付违约金；若因乙方质保不到位导致甲方或第三方损失，乙方需承担全部赔偿责任。

（5）乙方泄露本合同相关保密信息、小区业主信息或安防布局的，需向甲方支付合同总价款的10%作为违约金，若造成甲方或业主损失，需承担全部赔偿责任。

## 十、安全文明施工

1. 乙方施工人员需严格遵守小区安全管理规定及施工现场安全要求，佩戴安全防护用品，高空作业、电气作业等特殊岗位人员需持证上岗，严禁违规操作。

2. 乙方负责施工现场的安全管理工作，设置明显的安全警示标志，采取有效的安全防护措施，防止发生安全事故；施工过程中发生的人员伤亡、财产损失、第三方索赔等，均由乙方全部承担，与甲方无关。

3. 乙方需文明施工，保持施工现场整洁有序，施工垃圾及时清理，不得随意堆放、丢弃，施工过程中避免产生噪音、粉尘等污染，减少对院区正常工作的影响，施工时间需避开业主休息时段（建议施工时间：9：00-12：00，14：00-18：00）。

## 十一、知识产权与数据归属

1. 乙方提供的管理平台、系统软件等相关知识产权归乙方或品牌方所有，乙方授予甲方永久使用权，不得擅自收回授权、加价收取软件年费（本合同另有约定的除外）。

2. 本院区智能化系统产生的所有数据，其所有权、使用权均归甲方所有，乙方不得私自拷贝、外传、泄露、篡改上述数据，不得用于本合同约定以外的其他用途，否则承担相应法律责任及经济赔偿责任。

3. 乙方不得在系统中植入恶意程序、后门程序，不得擅自远程操控系统、获取系统数据，若发现乙方存在上述行为，甲方有权单方面解除合同，乙方需退还甲方已支付的全部款项，并按合同总价款的20%向甲方支付违约金。

## 十二、保密条款

甲乙双方对本合同的内容、合同价款、工程方案、设备清单、系统数据等相关信息承担永久保密义务，未经对方书面同意，不得向任何第三方泄露、披露或使用上述保密信息。本保密条款在本合同终止后仍具有法律效力，直至保密信息公开为止。若一方违反保密条款，需向对方支付合同总价款的10%作为违约金，若造成对方损失，需承担全部赔偿责任。

# 第三部分 通用条款

## 十三、不可抗力

1. 本合同所称不可抗力，是指不能预见、不能避免并不能克服的客观情况，包括但不限于地震、洪水、台风、暴雨、火灾、战争、政府政策调整等。

2. 因不可抗力导致本合同无法履行或延迟履行的，遭遇不可抗力一方应在不可抗力发生后 24 小时内通知对方，并在不可抗力发生后 7 个工作日内提供相关证明文件，双方互不承担违约责任，工期相应顺延。

3. 不可抗力发生后，双方应积极采取措施，减少损失，若因一方未及时采取措施导致损失扩大，扩大的损失由该方承担。

## 十四、争议解决

本合同履行过程中发生的任何争议，双方应首先友好协商解决；协商不成的，任何一方均有权向工程所在地人民法院提起诉讼。

## 十五、合同组成文件

本合同由以下文件组成，互为补充、互为解释，若存在冲突，按以下优先级排序：

1. 本合同协议书及专用条款、通用条款；

2. 附件一《供货清单及明细》；

## 十六、其他约定

1. 本合同一式肆份，甲方执贰份，乙方执贰份，自双方签字盖章之日起生效，具有同等法律效力，至工程竣工验收合格、质保金结清、双方权利义务履行完毕后自动终止。

2. 本合同未尽事宜，双方可另行协商签订书面补充协议，补充协议与本合同具有同等法律效力。

3. 双方的联系地址、联系方式为本合同履行过程中的有效送达地址，若一方变更联系地址、联系方式，需提前 3 个工作日书面通知对方，否则因此产生的送达不能、损失等，由变更方自行承担。

4. 本合同中的“书面形式”包括合同书、信件、传真、电子邮件等可以有形地表现所载内容的形式。

**签章页**

甲方（盖章）：_____

法定代表人/授权代表人（签字或盖章）：_____

日期：2026年11月9日

乙方（盖章）：_____

法定代表人/授权代表人（签字或盖章）：_____

日期：2026年11月9日

《供货清单及明细》

| 序号 | 产品名称 | 品牌及规格型号 | 生产厂家 | 是否中小企业产品 | 数量 | 单价 | 总价 |
|---|---|---|---|---|---|---|---|
| 1 | 漏洞扫描 | 迪普（Scanner1000-MA-G） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 2 | Web 应用防火墙 | 迪普（WAF3000-MA-G） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 3 | APT 攻击预警平台 | 迪普（APT1000-GC-G） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 4 | 入侵防御系统 | 迪普（IPS2000-MA-G） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 5 | 网络安全审计系统 | 迪普（UAG3000-MA-G） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 6 | 网络准入系统 | 联软（ LV-7050C） | 深圳市联软科技股份有限公司 | 否 | 1/台 | | |
| 7 | 统一管理平台 | 迪普（SW-UMC-PLAT） | 杭州迪普科技股份有限公司 | 否 | 1/套 | | |
| 8 | 安全接入网关 | 迪普（LSW5620-24GT4XGS） | 杭州迪普科技股份有限公司 | 否 | 1/台 | | |
| 9 | 实施安装调试 | 定制 | 陕西亿弘通电子科技有限公司 | 否 | 1/项 | | |