

千阳县人民法院网络安全设备采购项目

施 工 合 同 书

(甲方) 采 购 人： 千阳县人民法院

(乙方) 中标供应商： 陕西柏云电子科技有限公司



千阳县人民法院网络安全设备采购项目施工

合同书

(甲方) 采 购 人：千阳县人民法院

(乙方) 中标供应商：陕西柏云电子科技有限公司

一、项目名称：千阳县人民法院网络安全设备采购项目（项目编号：
SXMRYC2024-1081 号）

二、合同构成：下列文件构成本合同不可分割的组成部分，与本合同具有同等法律效力：

1. 本合同书；
2. 中标通知书；
3. 招标文件及澄清、修改、补遗文件；
4. 乙方的投标文件及书面澄清、说明、补正文件；
5. 产品的说明书、合格证、检测报告等有关资料；
6. 产品验收报告单；
7. 合同的其它附件。

三、合同标的：查看合同附件。

四、合同总价格：人民币（大写）壹拾肆万贰仟元整，（小写）¥:142000.00元。

五、交货时间、地点、方式、质保期

1. 交货时间：自合同签订之日起15日历日内完成供货并交付使用。
2. 交货地点：千阳县人民法院。
3. 交货方式：乙方负责将货物（产品）安全完好运抵交货地点、安装调试并保证验收合格。

4. 质保期：所有产品的质保期为验收合格后一年。

六、付款方式

甲方承诺全部货物（产品）安装并验收合格后，支付合同总价 142000.00 元（大写：壹拾肆万贰仟元整）。

七、质量保证

乙方提供的产品及材料必须保证质量可靠，进货渠道正常，配置合理齐全，应全面满足招标文件的要求，招标文件未明确要求的内容，乙方须按采购产品的主流标准配置或以甲方的补充要求为准。所供产品工艺质量应严格按国家最新发布的规范标准执行，如发生质量问题由乙方承担全部责任。

八、运输、安装要求

1. 乙方根据产品特性，自行选择运输及包装方式，承担一切运输费用包括从生产厂商到甲方指定交货地点所需的装卸、运输（含保险费）及其他一切费用。

2. 乙方应在合同规定的安装调试期内完成该项工作。如因乙方责任而造成延期，每超过一天按合同总价款的（5‰）支付甲方误期赔偿金，直至交货或服务结束为止，所有因延期而产生的费用由乙方承担。

3. 安装和调试期间所发生的费用均由乙方负责。

4. 乙方应对安装调试、整改等实施过程的安全负责，如发生人身伤亡财产损失的由乙方负责解决并承担全部责任。

九、技术支持、技术培训、技术资料

（一）、技术支持：

1. 提供保修期内全年 7×24 小时的技术咨询服务。乙方怠于或无法提供技术支持的，甲方有权委托第三方处理，由此产生的费用和后果由乙方负责，费用直接从应付款或质保金中扣除。乙方指定的项目总协调人必须是乙方公司管理层人员。货物使用过程中一旦出现重大问题，项目总协调人应能及时赶到现场。乙方更换项目负责人和主要技术人员，须将变更人及其工作影响、替换人资历等情况以书面材料报告项目甲方审核，经同意后方可更换。因乙方的人员变更原因所造成的任何项目质量、进度滞后的后果，由乙方承担。

2. 乙方在项目实施过程中，质量保障人员、资源不足或者执行不力，给项目质量带来的风险超出甲方认定的允许范围时，甲方可终止本项目合作并进行索赔。

(二)、技术培训：

应包括产品使用操作、保养、维修等培训内容。乙方需按甲方要求的时间为甲方免费培训技术人员若干名，培训服务以受培训人员熟练掌握相应技能为原则。在产品投入使用初期进行必要的跟踪指导，保障产品的稳定运行。投标产品需在培训基地培训的，乙方应按要求履行，培训产生的交通费、食宿费、培训费等均由乙方承担。

(三)、技术资料要求：

乙方应向甲方提供全套中文技术资料一套，其费用包括在磋商价格中：

1. 产品合格证、清单、说明书和维护、修理技术文件，图纸（线路图、原理图等）、保修卡等；

2. 制造厂的检验、测试报告、产品检验合格证书，质量保证书等文件验收时须一并提供；

3. 验收标准；

4. 技术说明书及必须的其它技术资料；

5. 安装、维修图及原理图；

6. 零部件目录；

7. 备品备件、易损件清单；

8. 项目完工后提供验收报告；

9. 合同中要求的其他文件资料。

十、验收：

由甲方和乙方共同对项目进行安装验收和最终整体验收。其内容包括确认产品的产地、规格、和数量等，对其产品性能参数、样式、颜色，以及质量是否达到现行国家有关验收规范“合格”标准、是否按照甲方要求进行安装到位、是否

在规定时间内安装完毕、所有产品的配套包装是否完好无损等进行逐项检查。

1. 所验产品的指标、性能参数最终验收达不到招标文件要求和响应文件承诺的，或在使用中发现甲方不能容忍的缺陷等，将视为产品验收不合格乙方应在甲方要求的时间内无条件免费更换或退货。

2. 若发现乙方有弄虚作假的，在投标阶段故意或随意夸大产品技术性能，乙方应无条件退货，本合同解除，乙方赔偿甲方相应的损失。

3. 验收标准：按招标文件、投标文件及澄清函等技术指标进行验收。各项指标均应符合验收标准及要求。

4. 验收合格后，填写验收单，双方签字生效。

5. 验收依据：

5.1 合同文本；

5.2 投标文件及澄清函、招标文件；

5.3 国家和行业制定的相应的标准和规范；

5.4 验收清单（注明各部件的品名、数量、规格型号和原产地或生产厂家）。

十一、质保及维保服务（提供售后服务承诺函）：

1. 在保修期内，乙方应提供可承担维修职能的公司、全资分公司或办事处，并驻守多名维护技术人员，并提供地点、联系人（常驻工程师）及联系电话（服务热线），随时解答各种疑问（需提供相关证明材料）。

2. 保修期内，由于乙方原因造成质量问题，乙方于接到甲方通知后 24 小时内派人维修，属甲方使用不当及其他非乙方原因造成项目质量问题，乙方可给予维修，但甲方须按不高于市场价格支付维修费。

3. 因乙方责任过失造成的设备质量问题，由乙方负责整改、维修。

4. 保修期内，设备出现故障后（因不正当使用、不可抗力因素除外），乙方须在接到甲方通知后 24 小时内到达现场负责对设备进行免费维修如乙方不尽履行保修义务，甲方有权委托其他单位进行维修，相应费用由乙方承担（从保证金中扣除，不足部分由乙方补交）。

5. 乙方必须确保设备的质量和安​​全，因乙方原因致使工程在合理使用年限内因质量或安全隐患和缺陷造成人身和财产损害的，乙方负责事后补救并承担全额赔偿责任。本款不受保修期的限制。

十二、知识产权

乙方应对所供产品具有或已取得合法知识产权，乙方应保证所供产品及服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由乙方负责解决并承担全部责任；如因此影响到甲方的正常使用，甲方有权单方解除本合同，乙方应无条件向甲方退回已收取的全部合同价款。

十三、违约责任

1. 按《中华人民共和国政府采购法》、《中华人民共和国合同法》中的相关条款执行。

2. 乙方逾期供货或未按合同或招标文件要求提供产品或提供的产品质量不能满足采购人技术要求的，甲方有权终止合同，要求乙方赔偿经济损失并承担违约责任。

3. 乙方的投标文件为签订正式书面合同书不可分割的部分，乙方应履行相应的责任。

十四、争议的解决方式：合同执行中发生争议的，当事人双方应协商解决，协商达不成一致时，可向项目所在地人民法院提请诉讼。

十五、不可抗力情况下的免责约定



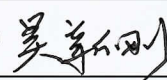
双方约定不可抗力情况指：双方不可预见、不可避免、不可克服的客观情况，（包括但不限于：战争、严重火灾、洪水、台风、地震等。）但不包括双方的违约或疏忽。

十六、合同份数：本合同正本一式肆份，供需双方各执贰份。

十七、合同生效：本合同在供需双方法定代表人或其授权代理人签字、加盖双方公章或者合同专用章。

十八、合同修改：除甲乙双方签署书面修改、补充协议外，本合同条件不得

有任何变化或修改。

甲方	乙方
千阳县人民法院（盖章）	陕西柏云电子科技有限公司（盖章）
地址：宝鸡市千阳县东大街 19 号	地址：宝鸡市渭滨区滨河南路 1 号渭滨区互联网产业园 1 号楼 1405 室
邮编：	邮编：721000
全权代表：（签字） 	法定代表人： 
	被授权代表：（签字） 
电话：	电话：0917-3254618
传真：	传真：0917-3254600
	开户银行：中国银行宝鸡陈仓园支行
	账号：102414997320
日期： 年 月 日	日期： 年 月 日

附件:

序号	货物名称	品牌	型号规格或主要技术指标	数量	单位	单价 (元)	总价 (元)
1	综合威胁探针系统	绿盟	<p>型号: UTSNX3-HD4100-P</p> <p>2U 机型</p> <p>SSD 为 64G</p> <p>硬盘为 24T</p> <p>管理口有 2 个 GE,</p> <p>console: 1 个 RJ45 接口, 8 个 10/100/1000M 电口, 4 个千兆 SFP 插槽, 扩展槽为 2 个,</p> <p>吞吐量为 1.5Gbps。</p> <p>包含流量采集、元数据提取、存储等功能</p> <p>流量采集:</p> <p>支持导入 HTTPS 证书, 对流量进行解密和还原; 支持流量白名单, 过滤掉不关注资产流量, 白名单类型应包括 IP、端口、邮箱、域名。</p> <p>威胁检测:</p> <p>★应覆盖多种攻击特征, 可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测, 攻击特征库数量至少为 9000 种以上。</p> <p>内置 WEB 应用机器学习检测模型, 支持对 sql, xss, exec, phprce, ptravel 和 jeli 攻击类型进行分类检测和告警, 告警信息至少包括机器学习告警类型和威胁事件名称。</p> <p>WEB 类告警详情中包含请求和响应信息, 在请求和响应信息中能标记规则匹配中的字</p>	1	台	142000.00	142000.00



	<p>段信息，便于运维人员快速进行确认攻击事件。</p> <p>内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。</p> <p>★支持自定义 TCP/UDP 行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称。回溯分析：</p> <p>应具备元数据提取、存储和检索的能力。</p> <p>★支持元数据存储和展示，元数据类型至少包括 TCP&UDP 日志、HTTP 日志、EMAIL 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志。</p> <p>响应：</p> <p>支持对入侵检测告警、WEB 应用告警、威胁情报告警和恶意文件告警中的攻击 IP 和受害 IP 发送阻断报文，进行旁路阻断。</p> <p>支持自定义一键封堵，配置策略包括 IP 类型（配置选项包括源 ip/源端口/目的 ip/目的端口）、域名类型、生效时间和失效时间。</p> <p>支持与大数据平台联动：提供 API 接口，由大数据平台通过接口下发一键封堵策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。</p> <p>取证（流量存储）：</p> <p>支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口、起止时间。</p> <p>支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的 payload 进行匹配。自定义规则内容至少包括：源 IP/源端口、目的 IP/目的端口、匹配类型（二</p>			
--	---	--	--	--



		<p>进制、字符串、正则表达式)、匹配特征、会话数量、过期时间。</p> <p>资产识别： 支持从流量中识别资产信息和展示，识别的信息至少包括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。</p> <p>动态沙箱检测： 支持样本虚拟化执行环境，具备 windowsxp、windows7、windows10 和 android 执行环境</p> <p>基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征（进行为，逃逸行为），分类识别各种加壳病毒及未知恶意代码；</p> <p>★可记录文件运行期间的注册表行为、文件行为、网络行为等所有行为记录。支持文件检测内容包含恶意文件来源，恶意行为类型，恶意文件进程操作，文件操作，网络操作，注册表操作等可疑行为。</p>			
<p>合计：(大写) 壹拾肆万贰仟元整</p>		<p>小写：¥142000.0 元</p>			