合同编号：ZJWZA2409123CGN00

苍南县网络安全服务保障中心建设项目合同

甲方：中共苍南县委宣传部

乙方：中国电信股份有限公司温州分公司

甲、乙双方根据《中华人民共和国政府采购法》《中华人民共和国民法典》和苍南县网络安全服务保障中心建设项目的采购文件相关规定，双方达成一致签署本合同。

一、项目内容

二、合同金额

本合同金额为（大写）：肆拾玖万叁仟伍佰元（￥493500元）人民币。

三、技术资料

1.乙方应按采购文件规定的时间向甲方提供有关技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给予履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

乙方应保证提供服务过程中不会侵犯任何第三方的知识产权。

五、转包或分包

1.本合同范围的服务，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的服务全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，甲方有权解除合同，并追究乙方的违约责任。

六、合同履行时间、履行方式及履行地点

1.履行时间：乙方在合同签订 10 日内提供完整的安全运营工作实施方案，包括对照运营目标列出具体的实施内容、计划，以及参与运营的人员名单等，经核验通过后启动运营服

务。

2.履行方式：服务期间通过采取动态考核方式进行日常评估，对达不到考核指标要求的，可对年度运营及服务费用进行扣减。所采购的运营服务期满后，经评估达到预期效果的，可通过采购提供持续服务。

3.履行地点：苍南县

七、服务期限

1.服务期限：2024年12月18日-2025年12月18日，服务期一年，第二年开始另行支付。

八、付款方式

（1）签订合同生效并具备实施条件后 7 个工作日内支付签约合同价的 40%作为预付款（采购人可根据项目特点、供应商信用等情况，确认是否要求供应商提交银行、保险公司等金融机构出具的预付款保函（见索即付）或其他担保措施）；

（2）提供完整的安全运营工作实施方案后支付签约合同价的 60%尾款。

九、税费

本合同执行中相关的一切税费均由乙方负担。

十、质量保证及后续服务

1．乙方应按采购文件规定向甲方提供服务。

2．乙方提供的服务成果。对达不到要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴重做：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶解除合同。

3．如在过程中发生问题，乙方在接到甲方通知后在__2___小时内到达甲方现场。

4．乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

十一、违约责任

1．甲方无正当理由拒收接受服务的，甲方向乙方偿付合同款项5%作为违约金。

2．甲方无故逾期验收和办理款项支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3．乙方未能如期提供服务的，每日向甲方支付合同款项的千分之六作为违约金。乙方超过约定日期10个工作日仍不能提供服务的，甲方可解除本合同。乙方因未能如期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值10%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

十二、不可抗力事件处理

1．在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2．不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3．不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

十三、诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

十四、合同生效及其他

1．本合同一式六份，经双方法定代表人或授权代表签字并加盖单位公章后生效。

2．合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签订书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3．本合同未尽事宜，遵照《民法典》有关条文执行。

合同编号：ZJWZA2409123CGN00

甲方(盖章)：中共苍南县委宣传部

委托代理人：

开户银行：

开户名称：

账号：

签约日期：

乙方（盖章）：中国电信股份有限公司温州分公司

委托代理人：

2024 年 12 月 17 日

开户银行：温州市工行营业部

开户名称：中国电信股份有限公司温州分公司

账号：1203202019905480254

签约地点：

附件：

序号	服务内容	单位	数量	单价（元）	合计（元）	备注
1	扫描检测	项	1	50000	50000	
2	事件调查	项	1	50000	50000	
3	7*24 小时云防护	项	1	93500	93500	
4	人员驻点2人	项	1	300000	300000	
总价合计（元）				493500		

No.	服务名称		服务内容	数量	单位
1	本地检测使用工具	明鉴漏洞扫描系统	1.漏洞扫描产品：安恒明鉴漏洞扫描系统（DAS-RAS）是一款建立在安恒多年信息安全漏洞挖掘、渗透测试技术研究和漏洞检查方法的最佳实践基础之上，集主机安全扫描、网站安全扫描、数据库安全扫描、弱口令发现和基线配置核查于一身，帮助用户提高网络安全防护性能和抗破坏能力的产品； 2.并发任务数：15个；DAS-RAS-BAS * 1；DAS-RAS-CVS * 1；DAS-RAS-DBS * 1；DAS-RAS-DIS * 1；DAS-RAS-WAS * 1；DAS-RAS-WSM * 1；DAS-RAS-IPLS04 * 1； 3.默认质保：三年	1	套
		应急处置工具箱	1.应急处置工具箱产品（适用于应急处置与应急处置演练）：1、对应急处置流程进行了优化，并全程指导应急处置步骤；2、同时提供丰富多样的取证手段与详尽的专家知识库，以满足不同场景下对应急处置工具以及相关知识的需求，实现了网络安全事件的取证溯源、快速恢复；3、一体化智能报表生成机制，自动涵盖整个应急处置流程工作内容，应急处置报告一键导出。 2.【软硬一体】其硬件规格（CPU 8核，内存32GB，硬盘 1TSSD）、网络接口（RJ45千兆网口 1个，USB端口3个，VGA或HDMI接口1个），屏幕14英寸，显示比例16：9，国产桌面版操作系统。 3.默认质保：三年	1	套
2	企业基础服务	企业资产梳理服务	协助梳理信息资产情况，对资产、业务系统、资产责任人进行关联，形成完整的资产信息台账，能清晰了解自身资产现状和资产分布。	1	套
		企业安全体检服务	基于各类检查工具的基础数据和基本执法检查流程，由服务人员对企业开展各类专项任务，如网络安全/等保专项检查、数据安全检查等		
		企业安全咨询规划服务	服务人员将以规划咨询的方式帮助企业构建一个全面、多层次的安全防护体系，将服务重点放在网络架构安全上，确保企业数据资产和业务流程的安全稳定运行。		
		企业安全培训服务	企业安全培训服务面向企业不同岗位人员进行定制化培训。服务可提供安全技能培训、攻防培训、认证培训等内容，可根据企业需求，定制安全培训服务内容。		
		协助企业安全加固服务	企业安全加固服务是依据安全体检、等保测评、安全评估等工作的结果，协助企业进行漏洞修复、脆弱性加固、网络架构整改等内容的服务。		
3	本地基础服务	人员驻场服务	通过提供“哨兵式”的网络安全看护服务，协助客户及时发现并有效控制网络安全风险和威胁，做到早发现、早处置，避免发生重大网络安全事件；提供“顾问式”的日常安全运维咨询和安全检查服务，为客户网络安全技术防护策略持续改进提供有效性安全建议。服务内容包括网络安全运行状态监测分析、网络安全告警分析和预警、网络安全风险和脆弱性检测、网络安全技术防护策略持续改进等服务内容。 1、网络安全运行状态监测分析：针对安全设备的性能、功能、硬件状态定期巡检，设立正常运行区间值、异常运行区间值、告警阈值，确保驻场人员能够及时发现异常并进行响应处置。 2、网络安全告警分析和预警：采用人工分析和机器辅助的方法，针对设备产生的网络安全告警事件进行分析、验证和处置。同时，利用人工对网络流量数据和日志进行主动、反复的检索，从而检测出逃避现有的安全防御措施的高级持续性威胁。 3、网络安全风险和脆弱性检测：通过安全防护策略梳理和验证、漏洞扫描、人工安全基线配置核查等手段，发现网络安全风险隐患和薄弱环节，提供网络安全修补和加固建议。 4、网络安全技术防护策略持续改进：针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全威胁和脆弱性，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，并定期开展策略配置备份、系统软件、特征库升级等操作。 5.协助做好上级网安部门下达的日常性网络安全工作事务，并做好重保时段应急值守等工作。	1	年/2人
		7*24小时云防护	提供零部署零运维云防护服务，分钟级接入，完成防通报、防黑、防泄露、防CC等安全防护。 玄武盾云防护包括CC防护、安全流量学习、已知攻击检查和未知攻击检查4大防护引擎，先通过专利级CC防护引擎进行识别及拦截，过滤扫描、爬虫、刷票、CC等应用层攻击。安全流量学习引擎采用机器学习算法对无害资源、正常访问行为、误报行为进行分析，通过一定的模型训练，将安全流量进行线速转发，提升应用层检测效率，针对剩余的非安全流量通过已知攻击检测引擎进行过滤，该引擎包括机器学习+规则双重检测算法识别并拦截注入、跨站、协议违规、Webshell、盗链、组件漏洞、CSRF、信息泄露等攻击。未知攻击通常危害大，隐蔽性强，采用威胁情报+虚拟补丁方式进行识别和拦截。	1	年/套
		安全意识培训	通过网络安全意识培训，对日益猖獗的病毒、木马等威胁进行必要的描述，使用户全体人员对网络安全的有初步的认识和逐步提高安全意识，并阐明具体的防范措施让安全事故可以得到有效的避免。	1	年/次
		应急演练	根据系统实际环境情况，提供多个场景下的演练方案，以模拟演练或者桌面推演的方式检验应急预案的完整性、可行性，提高应急处理能力。	1	年/次
		应急响应	根据事件类别，提供全年的应急响应服务，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。紧急事件主要包括：勒索病毒、病毒和蠕虫事件、黑客入侵事件、数据泄露、挖矿事件等。	1	年/次