



2025 年度柯桥区政务网络安全运营服务项目

临[2024]3967 号

合 同 文 件

甲方: 绍兴市柯桥区大数据发展管理中心

乙方: 联通(浙江)产业互联网有限公司

签订时间: 2025 年 2 月 24 日





合同协议书

甲方：绍兴市柯桥区大数据发展管理中心

乙方：联通(浙江)产业互联网有限公司

甲、乙双方根据 浙江翔实建设项目管理有限公司 项目编号为的 2025 年度柯桥区政务网络安全运营服务项目(临[2024]3967号) 项目的政府采购交易结果，签署本合同。

一、服务内容及标准

序号	服务名称	内容描述
1	安全运营服务-运营服务工具	包含监测中心、资管中心、感知中心、响应中心、Web 端工作台、浙政移动端等业务功能模块，构建覆盖“云、网、端、数据、应用”全链路安全技术防护能力，各维度数据通过大数据分析数据治理后进行汇聚整合，并进行统一安全管理，实现安全问题从“发现-解决”的闭环管理，含一名技术人员利用运营服务工具现场服务一年。
2	系统服务 一键封堵	将原有需要通过运营人员对各种安全设备的告警数据进行分析研判并手动处置的这一环节转换成剧本编排自动化的执行。主要将专业人员的分析经验沉淀为标准流程，不断优化响应策略，减少对人工的依赖，以剧本方式提前制定，并以流程化自动化完成事件管理及处置，将响应时间从小时甚至天降低到分钟级别。通过归集全量风险的汇聚，接入来自不同平台或设备的安全事件并对其进行解析处理，实现灵活的剧本编排，最大化人机结合程度，支持剧本与组件的自定义与统一管理配置，实现不同的方式触发剧本引擎产生相关案件，从而进行封堵恶意 IP 地址、禁止危险行为、阻断恶意流量等自动化响应处置联动。
3	服务器安全加固系统	针对服务器客户端，实现恶意代码防护、微隔离、云主机病毒查杀、防暴力破解、入侵攻击检测、勒索病毒、挖矿病毒检查实现统一的防范，同时提供主机防火墙、入侵检测、网络行为管控、安全基线、漏洞扫描等防护体系，全面覆盖黑客攻击阶段及各类威胁行为。包含一年更新服务、维保，包含 450 个点位/年，含一名技术人员利用运营



<p>4</p> <p>安 全 服 务</p>	<p>现场安全 服务</p>	<p>服务工具现场服务一年。</p> <p>1、业务上线前检测：针对首次上线区政务云或区政务信创云的业务系统，进行上线前检测，发现问题整改后复测，复测无安全隐患后准许系统上线。检测内容包含：高级渗透测试服务，人工渗透，在保证整个渗透测试过程都在可以控制和调整的范围之内尽可能的获取目标信息系统的管理权限以及敏感信息。针对发现的问题提出整改建议，并对整改结果进行人工核实；</p> <p>专项基线核查服务，根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具等专项检查方式，对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置等内容进行基线核查；软件代码安全检测服务，依据 OWASP TOP 10 等标准，通过工具扫描、高级安全专家人工确认、人工代码抽查等方式，对 Web 应用进行脆弱性（SQL 注入、跨站脚本等）、权限（权限控制不严格、表单逻辑处理错误等）、结构的安全检查，发现源代码中存在的安全风险。通过代码安全审计服务对系统源代码安全现状分析、定位源代码中存在的安全漏洞、评估漏洞风险、并提供整改建议。按照全区服务期内新上线区政务云或信创云系统数量提供服务。</p> <p>2、全区渗透测试服务：针对现有业务系统，定期由高级安全专家通过利用目标应用系统的安全弱点模拟黑客入侵攻击方法，以人工渗透为主，在保证整个渗透测试过程都在可以控制和调整的范围之内尽可能的获取目标信息系统的管理权限以及敏感信息。针对发现的问题提出整改建议，并对整改结果进行人工核实。模拟黑客攻击的手法，对指定信息系统开展全方位安全渗透，深度挖掘系统各层面安全漏洞，每月不少于 50 个系统。</p> <p>3、专项基线核查服务：针对现有资产，服务人员根据既定的检查规范及方法，通过现场人工和设备检查的方式，利用人工检查用表（checklist）、脚本程序或基线扫描工具对政务类、互联网等信息资产进行全面的安全配置核查和分析，包括主机系统安全、数据库安全、中间件安全等系统策略配置、服务配置、保护措施以及系统和软件升级、更新情况，发现配置的不合规项，每月不少于 50 台主机。</p>
-------------------------------------	--------------------	--



		<p>4、专项漏洞扫描服务：采用业界认可的、专业的扫描工具（不少于四个主流安全厂家工具），通过定制的扫描规则，形成安全扫描策略文档，对用户指定主机进行一次全面的自动化安全扫描，人工验证扫描结果，对误报漏洞进行修正，确保扫描结果的真实性后输出安全扫描报告及修复建议。漏洞扫描服务可以使客户了解当前技术措施是否有效执行，并通过及时修补完善，避免对信息系统造成严重影响，每月不少于 50 台主机。</p> <p>含一名技术人员利用不同厂家运营服务工具现场服务一年</p>
5	重大活动及应急响应保障服务	重大活动时期（两会、HW 等），提供具有大型网络系统安全保障经验、攻防经验的技术人员以现场值守方式提供安全保障工作，同时通过根据事件类别，通过远程或现场支持的形式协助大数据发展管理中心对遇到的突发性安全事件进行紧急分析和处理。
6	网络资产梳理	利用资产测绘能力，结合数据使用场景和业务属性，识别数据资产分布，定期梳理和更新网络资产，形成资产清单。
7	网络安全培训服务	组织开展本地区宣传教育及培训。1 年 2 次
8	攻防演练服务	组织攻击队伍参加的网络攻防实战演习 1 次，在真实的互联网络环境下，组织不少于 8 个攻击队伍模拟黑客组织对提供的各类单位目标系统进行网络攻击，试图非法入侵。

二、服务价格

序号	服务内容		数量及单位	综合单价(元)	合价(元)
1	系 统 服 务	安全运营服务-运营服务工具	1 套/年	440000.00	440000.00
2		一键封堵	1 套/年	160000.00	160000.00
3		服务器安全加固系统	1 年	375000.00	375000.00
4		现场安全服务	1 年	250000.00	250000.00
5		重大活动及应急响应保障服务	30 人/天	85000.00	85000.00



6	务	网络资产梳理	1 年	30000.00	30000.00
7		网络安全培训服务	1 年	6000.00	6000.00
8		攻防演练服务	1 次/年	140000.00	140000.00
<p>合计金额大写: 人民币壹佰肆拾捌万陆仟元整 小写: ¥:1486000.00</p>					

三、技术资料

- 乙方应按采购文件规定的时间向甲方提供与本项目有关的技术资料。
- 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、样品或资料提供给与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。
- 乙方需承诺严格遵守绍兴市柯桥区大数据发展管理中心网络和数据安全相关工作要求,落实网络和数据安全责任,签订合同时同时签订相关网络和数据安全责任书。

四、知识产权

- 乙方应保证所提供的货物与服务均不会侵犯任何第三方的知识产权。
- 乙方保证所交付的货物及服务的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。
- 乙方承诺保护甲方在使用合同产品或其任何一部分时不受第三方提出侵犯专利权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控,由乙方负责与第三方交涉并承担可能发生的一切费用和相关法律责任,甲方不承担由此引起的一切经济 and 法律责任。

五、履约保证金

- 履约保证金: 无。

六、项目服务期限及实施地点

- 服务期限: 1 年,自甲方组织项目初验通过之日起算。
- 实施地点: 绍兴市柯桥区,具体事项须按甲方要求执行。



七、付款

本项目合同总价为人民币壹佰肆拾捌万陆仟元整（小写：¥1486000.00）。

1、第一期付款：合同签订后，经甲方确认且收到乙方合规发票，7个工作日内支付合同价的40%，即人民币伍拾玖万肆仟肆佰元整（小写：¥594400.00）。

2、第二期付款：服务所需所有软件系统安装部署完成，甲方组织专家初验合格后开始计算服务期，一年运营服务期满后，甲方组织专家验收合格后且收到乙方合规发票7个工作日内支付合同金额的60%，即捌拾玖万壹仟陆佰元整（小写：¥891600.00）。

乙方未按照合同预定的时间及要求履约的，或未达到合同规定的质量要求的，甲方有权暂缓支付合同款；

发票应随付款进度同时提供（乙方按照国家有关规定缴纳相应税费）。

因财政审批流程耗时导致付款延误的，不视为甲方违约。

八、税费

本合同执行中相关的一切税费均由乙方负担。

九、验收要求、标准

1、验收以采购文件和技术文件、投标文件、合同及安装技术要求为依据。

2、验收必须符合国家、地方有关规范、标准及设计要求。

3、符合验收条件的，由甲方组织专家按照国家、地方有关规范、标准及设计要求进行验收。验收后乙方应按照验收中提出的意见整改。

4、整改完毕且复验合格后将货物服务交给甲方使用，完成日期以通过复验日期为准。

5、甲方在乙方服务过程中，如果发现服务内容数量不足或有质量、技术等问题，乙方应负责根据合同及甲方的要求采取补足或更换等处理措施，并承担由此发生的一切损失和费用。

十、售后服务

乙方需提供专门的售后服务电话10010，乙方在接到甲方通知后，1小时内做出响应，4小时内派人赴现场处理问题。24小时内无法修复的，乙方需提供无偿提供备机或备用零件供甲方使用。

十一、技术培训



1、在项目组织初验之前，应完成对甲方操作人员的培训（提供完整的技术培训，使甲方今后能自行操作、基本的维护）。

2、乙方应分别提供称职的指导人员，为甲方确定的培训人员在现场提供操作和维护培训。

3、乙方应编写培训手册并取得甲方同意，本手册应是根据本项目的货物或服务，在有关测试、操作及维护方面，对人员的培训和指导提供全面的培训手册，每种手册提供六套。如果需要，甲方有权对其进行复印，并不受限制的使用、分发该手册。

4、乙方应对甲方提供全面的技术和维护咨询。

十二、数量调整

甲方保留合同履行中调整部分服务的权力，乙方应对服务类别明细报价，按投标单价不变的前提下进行调整，双方不得拒绝。合同最终结算金额按实际使用量乘以投标单价进行计算，追加的采购金额不得超过原合同采购金额的10%。如遇本次招标没有涉及的服务时，由乙方提供申请，甲方确认后实施。

十三、违约责任

1. 甲方无正当理由拒绝验收项目的，甲方向乙方偿付拒收合同总价的百分之五违约金。

2. 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。因财政审批流程造成甲方付款延迟的，不视为甲方违约。

3. 乙方逾期提供服务的，乙方应按逾期交付项目总额每日千分之六向甲方支付违约金，由甲方从合同款项中扣除。逾期超过约定日期10个工作日不能交付的，甲方可解除本合同。合同解除后，乙方应返还已收取的费用。乙方因逾期交付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5%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。

4. 乙方所履行的服务质量或服务数量不符合合同规定及采购文件规定的，甲方有权中止接受服务，单方面解除合同，且相关损失由乙方承担。

5. 解除合同应按《浙江省政府采购合同暂行办法》向财政备案。

十四、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。

十五、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。

十六、合同生效及其他

1. 合同经甲、乙双方签名并加盖单位公章或者合同专用章后生效。

2. 采购文件、投标文件与本合同具有同等法律效力。

3. 本合同未尽事宜,遵照《民法典》有关条文执行。

4. 本合同一式五份,具有同等法律效力,甲、乙双方各执二份,采购代理机构一份。



(以下无正文, 为 2025 年度柯桥区政务网络安全运营服务项目合同之签署页)

甲方(盖章): 绍兴市柯桥区大数据发展管理中心

地址: 浙江省绍兴市柯桥区群贤路 1661 号

法定(授权)代表人:

签名日期: 2025 年 2 月 24 日



徐晓

乙方(盖章): 联通(浙江)产业互联网有限公司

地址: 浙江省杭州市临平区南苑街道玩月街 101 号 2 幢 19 层

开户行: 中国工商银行杭州羊坝头支行营业室

开户账号: 1202020119900326629

法定(授权)代表人:

签名日期: 2025 年 2 月 24 日



胡鸿基



附件一： 2025 年度柯桥区政务网络安全运营服务项目应用信息技术服务外包单位网络安全承诺书

绍兴市柯桥区大数据发展管理中心：

为确保我单位开发/运维的绍兴市柯桥区大数据发展管理中心 2025 年度柯桥区政务网络安全运营服务项目 系统安全稳定运行，我单位郑重承诺认真落实绍兴市柯桥区大数据发展管理中心部署的各项网络安全工作任务，采取包括增加人员和经费投入在内的一切必要手段，确保系统安全运行，确保不发生网络安全事件。

我单位明确：沈丹斌为我单位项目负责人，全面负责信息系统管理和网络安全工作，派出骨干技术力量负责项目的开发、运维和保障工作。我单位将把应用系统安全运行情况纳入对上述人员的奖惩考核范围并充分征求贵单位意见。

我单位承诺：按照国家法律法规和技术标准加强网络安全技术防护，确保自身和相关供应链的网络安全，积极配合贵单位和国家涉网监管部门组织的检查、检测等工作。与贵单位官方网络安全服务合作伙伴做好技术对接，确保重要网络安全态势信息互联互通。按照最小化原则管理相关权限、信息和数据，对重要信息系统原则上采用双因子认证进行身份认证和授权访问。做好日常监测、技术巡检等工作，及时修复高危漏洞、关闭高危端口，配备防范页面篡改、黑客攻击、病毒入侵、系统故障、数据泄露等情况的技术力量，确



保系统安全稳定运行。制定应急预案,并定期开展应急演练,当发生网络安全事件时,应于24小时内向贵单位书面反馈突发网络安全和数据安全事件处置情况。留存系统日志、应用日志和行为审计日志等直至项目结束,确保网络访问行为可记录、可追溯。系统运行结束后按照贵单位的要求处置相关数据,确保系统安全关停。

我单位确认:已对该项目暴露在互联网上的系统测试账号、配置文件、系统数据、测试环境、试运行环境、密码记录、源代码(包括github、gitlab等)、弱口令、技术方案等与项目安全运行无关的信息进行了清理。后续也将对上述信息进行有效管理。

如我单位承建信息系统或我单位人员发生任何网络安全事件引发任何损失,我单位将采取一切可能的措施配合贵单位积极开展处置,承担相应损失,并追究相关人员责任。

单位名称(章):

2025年2月24日





附件二： 2025 年度柯桥区政务网络安全运营服务项目 应用信息技术服务人员网络安全承诺书

(绍兴市柯桥区大数据发展管理中心、联通(浙江)产业互联网有限公司):

本人已认真阅读并将持续学习《绍兴市柯桥区大数据发展管理中心网络安全管理办法》等网络安全管理规程和政策流程文件。本人对个人掌握的信息系统权限负责，不向他人泄露或共享本人所有的系统权限。提升安全意识、注重用网安全，确保本人管理的权限、账号以及计算机终端安全。如工作岗位发生调整，本人将及时做好必要的交接程序。

本人承诺:遵守《网络安全法》《数据安全法》《保密法》等国家法律法规及标准规范，遵守项目组和单位的各项网络安全管理制度和工作要求，认真做好技术服务和保障工作，确保信息系统安全稳定运行。及时向项目组报告信息系统的重大变更、重要操作、运行态势等重要信息，积极配合各类网络安全检查、检测和演练工作，确保不发生网络安全事件。

本人同意:把绍兴市柯桥区大数据发展管理中心政务安全运营中心项目应用安全运行情况纳入本单位对本人的奖惩考核范围。如我单位承建信息系统发生任何网络安全事件引发任何损失，本人将采取一切可能的措施积极开展处置。

承诺人(签字): 沈丹斌

2025 年 2 月 24 日