常州市政府采购合同（服务）

项目名称：常州人社保障中心 2026 年设备运维、网络安全服务及驻场服务项目

项目编号：JSZC-320400-JZCG-G2026-0257

甲方：（买方）常州市人力资源和社会保障公共服务与技术保障中心

乙方：（卖方）常州市同济科技有限公司

甲、乙双方根据常州市政府采购中心常州人社保障中心 2026 年设备运维、网络安全服务及驻场服务项目（采购包 1）公开招标的结果，签署本合同。

一、合同内容

1.1 标的名称：常州人社保障中心 2026 年设备运维、网络安全服务及驻场服务项目

1.2 标的质量：乙方提供的服务应符合国家、地方及相关政府管理部门和行业与本项目有关的各项服务标准、规范、规章要求，并满足甲方实际需求。

1.3 标的数量（规模）：

(1)负责对常州人社保障中心 PC、打印机、金保外设等终端设备硬件、操作系统、应用软件及基础网络设备的日常运维备份及运行环境的日常巡检、报警情况上报(杀毒防黑、日志、状态检查)等工作；硬件设备的定期巡检、保养(至少每月一次，并提交巡检报告)；(2)网站及应用 APP 的安全防护及巡检工作(至少每月一次，并提交巡检报告)；(3)硬件设备(防火墙、视频会议视讯设备等)运行环境的日常巡检工作，做好巡检记录；(4)视频会议的运维保障，需提前做好会议安排保障工作，随时配合软件开发公司进行系统联调，并做好相关调试记录；(5)定期形成各类巡检维护报告及年终服务报告；(6) 配合安全机构每年的例行安全检查，做好相关安全检查报告；(7)根据机房管理要求进行设备的搬运、安装；(8)运行环境现场故障处理，包括故障分析、恢复及维修；(9)提供运行环境硬件设备的备品备件及相关更换服务；(10)根据实际工作需求，向用户方提出新增的零配件名称、品牌、型号和价格等要素的采购建议报告；(11)根据用户方需要，向用户方信息管理人员开展技术培训，提供各类技术资料；(12)免费提供其他相关咨询服务。

（2）对 www.czrsj.cn 网站和应用的安全防护和服务。以及为 www.czrsj.cn 配置 SSL 安全防护证书，实现数据信息在客户端和服务器之间的加密传输，防止数据信息的泄露，保证双方传递信息的安全性。

1.4 履行时间（期限）：2027 年 1 月 1 日-2027 年 12 月 31 日

1.5 履行地点：常州市天宁区锦绣路 2 号

1.6 履行方式：配备 1 名服务工程师常驻现场；主动加强对 www.czrsj.cn 网站和应用的实时动态防御，保障网站群内各网站的安全，建立常态化监测防御、预警通知与应急保障，为网站起到 Web 安全防护、攻击溯源、安全加速和抗 DDoS 和抗 CC 攻击的作用，提升现有安全防护体系的能力：同时针对互联网各类型攻击防护，攻击工具识别、WebShell 防护、防御联动、Web 防火墙功能、后台锁、防盗链、缓存黑白名单等能够有效防护；增加实时攻击预警和通知服务，使网站管理和维护人员能够实时获取平台站群内所有网站的安全状况；实现在线网站安全专家的 7*24 小时应急响应，以及发生网络安全事件时进行驻场服务。

二、合同金额

2.1 本合同金额为（大写）：壹拾伍万捌仟元整（158000 元）人民币。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的货物）的有关技术资料。

3.2 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。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

本项目不收取履约保证金。

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

八、合同款项支付

8.1 分期付款：合同签订后，预付款支付比例：合同金额的 90%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。尾款支付时间：服务到期并验收通过，尾款支付比例：合同金额的 10 %。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

10.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验

收时，甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

10.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供服务的，甲方向乙方偿付拒绝接受服务合同价款总值__5%__的违约金。

11.2 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二向乙方支付违约金，但累计逾期付款违约金不超过逾期金额的百分之五。

11.3 乙方逾期提供服务的，乙方应按逾期提供服务合同总额每日千分之六向甲方支付违约金，由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工作日不能提供服务的，甲方可解除本合同。乙方因逾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价款总额__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。

11.4 乙方所提供服务的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

十二、不可抗力事件处理

12.1 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。

12.2 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。

12.3 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、解决争议的方法

13.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。守约方为解决争议所产生的各项费用(包括但不限于诉讼费、公证费、律师费、鉴定费、差旅费、保全费、担保费等)均由违约方承担。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

14.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

14.3 本合同正本一式两份，具有同等法律效力，甲方、乙方各执一份。

甲方：常州市人力资源和社会保障公共服务与技术保障中心

地址：常州市天宁区锦绣路 2 号

法定代表人或授权代表：

联系电话：

乙方：常州市同济科技有限公司

地址：常州市天宁区劳动西路 21 号 3 幢 1201 室

法定代表人或授权代表：

联系电话：0519-86697390

签订日期：2026 年 10 月 9 日

附件二、外包网络安全协议

外包网络安全协议

甲方： 常州市人力资源和社会保障公共服务与技术保障中心

乙方：常州市同济科技有限公司

一、协议依据及类型要点

根据《中华人民共和国民法典》及《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律法规及规范性文件的规定，甲(委托单位)、乙(承包单位)双方经协商一致，就⑨的服务项目(可选填：①建设信息系统或云平台<以下统称"信息平台">;②运维信息平台；③检查、监测、测评信息平台；④采购使用云计算服务；⑤采用社会网络平台提供对公服务；⑥采用社会网络平台发布政务信息；⑦采用社会网络平台实施社会管理；⑧采用社会网络平台处理党政事务；⑨其他信息技术)(以下简称"本服务项目"),签订本网络安全协议。

二、甲方的权利和义务要点

1.本服务项目中产生的政务数据、系统运行数据及收集的个人信息等数据资产(以下简称"外包数据资产")归甲方所有并可以随时在相关法律法规规定的范围内访问、利用、支配，在服务项目终止时有权要求乙方销毁或转移相关数据资产。

2.甲方建立对本服务项目的常态化网络安全监督管理，有权采取随机抽查、派驻人员或委托第三方机构等方式，对本服务项目网络安全管理情况开展常态化检查评估，通报问题隐患，责令限期整改；乙方应配合检查并及时整改。

3.甲方应提供乙方必要的工作条件，并按照最小必要原则授予乙方提供服务所需的相应权限，授权期满后及时收回相关权限，乙方应予以协助配合，不得设

置后门程序或者恶意程序。

4.在接受服务过程中，甲方发现乙方存在如下情形之一，导致合同继续履行将损害国家利益和社会公共利益的，甲方有权单方终止合同，且仅支付乙方相应服务期限内合理费用的80%(注：划线部分自行协商确定);乙方应及时返还多收取的价款(如从履约保证金中扣除):

(1)乙方规模能力、经营范围、资本构成、高管背景、技术水平、安全团队以及企业信用等方面发生重大变化，可能造成本服务项目存在重大网络和数据安全风险的;

(2)乙方(含相关工作人员及委托服务的第三方)因涉嫌违反网络安全、数据安全和个人信息保护相关法律法规，正接受有关主管部门立案调查(乙方应主动告知甲方该情况),甲方经评估后认为，乙方继续本服务项目可能存在重大网络和数据安全风险的;

(3)因乙方对服务合同中约定的网络和数据安全保护措施建设、使用不到位等，导致发生网络和数据安全事件，造成重大影响，或者产生网络和数据安全风险隐患被省级以上有关主管部门通报的;

(4)乙方违反本协议的约定、承诺或保证，尚未造成严重后果，甲方责令限期整改，乙方拒不整改或者整改不到位的。

5.在接受服务过程中，甲方发现乙方存在如下情形之一，导致合同履行将损害国家利益和社会公共利益的，甲方有权单方终止合同，并要求乙方返还全部合同价款，同时追究乙方的法律责任；乙方应及时返还已收取的合同价款:

(1)在服务合同签订前的三年内，乙方因违反网络安全、数据安全和个人信息保护相关法律法规，受到过行政处罚、刑事处罚，或者仍在接受有关主管部门

立案调查，但未主动告知甲方该信息的，被甲方通过其他方式获知的；

(2)乙方在本服务项目中的相关管理人员、操作运维人员经公安或国安部门背景审查存在问题，甲方要求乙方更换相关人员，乙方拒不更换的；

(3)违反网络安全、数据安全和个人信息保护等相关法律法规，拒不按照甲方要求改正、补救的。

(4)违反网络安全、数据安全和个人信息保护相关法律法规的规定，或者违反本协议的约定、承诺或保证，导致本服务项目发生重大网络和数据安全事件，或造成其他严重后果的。

三、乙方的权利和义务要点

1.在签订服务合同前，乙方应向甲方如实、完整提供其规模能力、经营范围、资本构成、高管背景、技术水平、安全团队、信用等级等经营管理信息，以及近三年因违反网络安全、数据安全和个人信息保护有关法律法规而受到约谈、行政处罚或刑事处罚等信息；未经乙方同意，甲方不得公开或向第三方提供相关信息。

2.乙方应当严格按照网络安全、数据安全和个人信息保护相关法律法规、国家标准及政策文件的规定提供安全可靠的产品、平台或服务，确保网络系统运行安全及相关数据资产的保密性、完整性、可用性；对在服务过程中接触到的甲方工作信息及相关文件，应予以严格保护，不得对外提供、公开、泄露或利用。

3.乙方应建立相对独立的管理技术团队，具体提供服务的相关人员应为乙方正式员工，并指定网络安全负责人。

4.乙方不得转包合同任务；确需分包的，应报经甲方同意，并在分包合同中明确相应的网络安全义务和责任，但不得对合同任务主体和关键部分进行分包。

5.乙方应严格按照法律法规规定及服务合同约定，收集、使用、存储、处理

数据和个人信息。

6.乙方应采取必要技术措施防范甲方所属数据资产的泄露、流失和违规操作。

7.乙方应将政务数据与其他数据分开存储、处理，未经甲方同意，不得变更用途、用法，不得访问、修改、公开、披露、利用、转让、销毁、私自留存或向第三方提供。

8.乙方在本服务项目中涉及采购相关产品和服务的，应当严格遵守如下规定要求：

(1)建设政务信息平台的，应当优先采用安全可信的软硬件产品；确无相关安全可信产品的，应当研究制定针对性措施防范安全风险；

(2)建设云平台的，应当选择供应链来源可靠的云平台管理软件、业务系统以及服务器 CPU、操作系统、数据库等；

(3)使用云计算服务(含 PaaS、IaaS、SaaS 等)的，应当按要求采用安全可信的云计算服务，并明确云服务商的网络和数据安全责任；

(4)使用商用密码的，应当符合国家密码管理规定。

9.乙方发现本服务项目中存在网络安全漏洞、缺陷或其他严重网络安全风险，应及时向甲方报告，或者直接向同级网信、公安部门报告；未经网信或公安部门同意，不得公开或向第三方提供。

10.乙方应严格落实相关开放性、兼容性标准和规范要求，优先采用通用系统解决方案，避免采用特定的技术架构、应用接口、数据格式等，确保系统的开放性和可移植性。

11.乙方发生业务转型、合并重组、投资并购等重大事项，或者管理技术团队人员发生重大变更，应提前向甲方报告。

12.乙方建设、运维的政务信息平台注册用户超过 100 万人或者涉及人民群众出行、教育、求职、医疗、缴费等重要业务，乙方应每年向甲方提交网络安全报告，报告至少包括网络安全管理、数据安全管理、平台关键软硬件安全、管理技术团队变化等情况。

13.乙方应建立外包服务项目安全管理工作规范，明确本单位及相关工作人员的网络安全责任，不断提升网络安全防护能力水平；定期组织本服务项目相关人员开展网络安全培训，规范安全操作规程，增强安全风险意识。

14.本服务项目终止时，乙方应配合甲方销毁或转移相关数据，并向甲方提供《网络安全承诺书》,承诺采取必要措施保证相关数据不可恢复，不私自留存、非法买卖或提供给第三方，不公开、披露、利用服务中知悉各类信息，否则乙方应承担一切法律责任。

15.因乙方提供外包服务导致甲方产品或服务存在安全隐患，乙方应采取有效措施予以补救，最大限度地降低影响范围。

16.乙方应积极配合网信、公安、审计、保密、密码管理等部门开展网络安全检查、测评、审计等监督管理工作，如实、完整提供相关网络安全管理情况，不得拒绝、隐匿、瞒报。

四、违约责任要点

1.乙方违反网络安全、数据安全和个人信息保护相关法律法规，或者违反本协议的约定、承诺或保证的，甲方有权追究乙方责任，乙方应按服务合同总价款的 10%或人民币 1 万元的金额(以两者中较高的金额为准)向甲方支付违约金；如造成甲方损失的，乙方应当全额赔偿。

五、争议解决要点

本协议履行期间存在争议的，双方协商解决；无法协商的，双方均有权向甲方所在地人民法院起诉。守约方为解决争议所产生的各项费用(包括但不限于诉讼费、公证费、律师费、鉴定费、差旅费、保全费、担保费等)均由违约方承担。

六、协议期限要点

与服务合同起止期限相同，但相关法律法规规定的网络和数据安全责任义务不受该期限的限制。

甲方（盖公章）：常州市人力资源和社会保障公共服务与技术保障中心

单位地址：常州市天宁区锦绣路 2 号

法人代表或委托代理人：

乙方（盖公章）：常州市同济科技有限公司

单位地址：天宁区劳动东路 11-18 号银河湾数码城 3 号楼 1201

法人代表或委托代理人：