常州人社保障中心设备运维、网络安全服务及驻场服务项目

采购包4合同

项目名称：常州人社保障中心设备运维、网络安全服务及驻场服务项目采购包4

项目编号：JSZC-320400-JZCG-G2026-0257

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：中国移动通信集团江苏有限公司常州分公司

根据常州市政府采购中心2026年9月11日进行的JSZC-320400-JZCG-G2026-0257号招标结果，甲、乙双方就乙方中标的常州人社保障中心设备运维、网络安全服务及驻场服务项目采购包4所涉及的有关问题，经过多次协商，达成一致意见签订合同。合同具体条款如下：

一、货物及其数量

常州人社保障中心设备运维、网络安全服务及驻场服务项目采购包4（项目编号：JSZC-320400-JZCG-G2026-0257）清单及价格。详细清单如下。

序号	服务名称	服务内容	单位	数量	单价	总价
1	网络安全流程规范体系服务	全面梳理常州市人力资源和社会保障公共服务与技术保障中心网络安全工作机制、职责以及相应流程规范体系	项	1	10000	10000
2	安全检查服务	漏洞扫描服务	次	12	1500	18000
		渗透测试服务	次	4	13000	52000
		系统上线前评估服务	项	1	6000	6000
		安全配置检查服务	次	4	2000	8000
		防守报告服务	项	1	6000	6000
		安全通报服务	项	1	3000	3000
3	网络安全风险防范与处置服务	带安全设备为常州市人力资源和社会保障公共服务与技术保障中心提供网络安全风险防范服务，避免或减少被主管单位的网络安全事件（僵木蠕、APT攻击等事件）通报。另外少量的安全事件通报应支撑甲方及时接收、处置并反	项	1	20000	20000

		馈市委网信办相关漏洞与网络安全事件通报				
4	政务信息化项目网络安全管理	对新建、改建、扩建政务信息化项目符合网络安全事前审核要求，配合开展相关工作。含以前自然年经审核项目符合事后检查要求。	项	1	8000	8000
5	网络数据安全管理	针对一个典型系统，落实国家数据分类分级保护制度规定，建立样板，指导其他网络数据准确识别、及时报送重要网络数据目录信息，持续加强数据安全保护;针对上述典型系统，组织开展1次数据安全风险评估。根据《常州市数据安全管理规范指南》指导，从管理和技术层面落实个人信息保护要求;指导督促向境外提供数据的数据处理者依法申报数据出境安全评估、订立个人信息出境标准合同;排查人社局下属单位，违法违规收集使用个人信息专项治理、人脸识别技术应用安全监督检查等。	次	1	38000	38000
6	完善保障体系	资产梳理：完善网络安全监管平台的资产信息，动态更新维护资产情况；落实政务信息化项目建设网络安全管理相关规定，对政务信息化项目网络安全“三同步”做好自查；按照《互联网政务应用安全管理规定》、《机关事业单位网络身份管理办法（试行）》等要求，落实网络身份管理任务，开展网络身份凭证（电子证书）申领、规范网上标识加注等工作；落实外包网络安全管理要求，开展外包管理风险排查，强化外包管理，依据《江苏省关于加强党政部门数字化建设中外包活动网络安全管理实施意见》要求，协助开展外包管理。防范因外包人员不当行为引起的重大失泄密案件和网络安全事件。	项	1	8000	8000
7	开展宣传教育培训	培训周期：每年提供一次（安全产品或者信息安全意识方面）提供与常州市人力资源和社会保障公共服务与技术保障中心业务环境密切相关的网络安全教育及意识培训，以提高员工的网络安全防护意识，进一步提高常州市人力资源和社会保障公共服务与技术保障中心网络的安全防护等级和水平。	次	1	2000	2000

中国移动通信集团江苏有限公司

8	网络安全周活动支撑服务	网络安全攻防实战演练服务 安全周活动配合	次	1	8000	8000
9	咨询服务	配合常州市人力资源和社会保障公共服务与技术保障中心在网络安全规划与建设、数据安全规划与建设中提供安全咨询服务、产品选型、合理化建议等。数据安全咨询服务：根据中心数据安全信息化发展需求，协助用户做好数据安全网络安全建设的整体规划设计，安全集成项目、数据安全相关事宜的前期方案咨询、中期实施跟踪及后期验收及维护服务。	项	1	5000	5000
10	其他安全服务内容	配合常州市人力资源和社会保障公共服务与技术保障中心完成市委网信办相关单位考核的相关内容。	项	1	5000	5000
投标总报价（人民币：197000 元）						197000

二、合同金额

本合同最终成交金额为人民币：**壹拾玖万柒仟元整（￥）（小写197000元）。**

三、服务承诺：

乙方公司为甲方突发事件提供 7×24 小时技术支持，对于突发事件，乙方公司在 1 小时内到达现场。服务内容包括对信息系统的安全渗透服务、网络安全攻防实战演练服务、安全检查服务、安全咨询服务、安全应急响应服务等。

四、项目实施进度

履行地：常州市人力资源和社会保障公共服务与技术保障中心

服务期限：2027年1月至2027年12月

五、技术情报和资料的保密

甲乙双方在合作过程中对对方所透露的或履行合同所知悉的技术、信息等均需承担保密责任，未经双方书面允许，任何一方不得向第三方泄露。并采取一切合理和必要措

施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。本保密义务的期限，从一方知悉该信息或资料之日起，直至公众可通过合法途径获得、知悉相关信息或资料之日止，并不因合同履行完毕而终止。

六、风险责任的承担

1、甲方承担协调风险责任，即甲方在提供业务需求的过程中因甲方的协调因素，造成项目不能完成或不能如期完成的，由甲方承担全部责任。

2、乙方承担技术风险责任，即技术能力因素造成项目不能完成或不能如期完成的，乙方承担全部责任。

3、因火灾、洪水、地震等不可抗力因素造成项目延误的，双方本着平等互利的原则，根据实际情况另行订立合同。

七、双方责任

（一）甲方责任：

1、甲方有义务按本协议按时付款；

2、在服务期间，甲方应做好配合工作，对于甲方未按乙方要求予以必要的配合，由此给服务造成的不利影响和后果，乙方不承担任何责任。

3、对于乙方服务进行监督并要求乙方在限定期限内整改。

（二）乙方责任：

1、乙方应按照本协议内容和要求提供相关服务。

2、乙方在服务过程中，有义务和甲方就项目方案，实施计划等和甲方充分进行沟通，并积极听取甲方的意见。

3、履行本合同过程中形成的书面报告的知识产权属于甲方所有，未经甲方书面同意，乙方不得用于本合同外其他目的。

4、乙方负责解决工作人员的劳动纠纷，在合同有效期内解除劳动合同等纠纷均由乙方负责处理并承担相应法律责任。如发生工伤、疾病、各类事故乃至死亡的一切责任及费用全部由乙方负责，乙方应严格遵守国家有关的法律、法规及行业标准。

5、因乙方工作人员原因造成工作人员自身、乙方、甲方等人身或财产损失的，均由乙方承担赔偿等法律责任，甲方不承担任何法律责任。

6、积极响应甲方提出的整改意见，不断完善服务。

八、验收标准和方法

1、乙方完成技术服务工作的形式：乙方提供《年度技术服务报告》，其内容包括现场服务报告，系统设备维修更换清单等技术文档。

2、技术服务工作成果的验收标准：全年系统运行是否正常、乙方技术人员现场服务质量以及各种报告的质量是否符合甲方要求。

九、付款方式

1、预付款支付时间：合同签订后10个工作日内，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。

2、尾款支付时间：服务到期并通过考核，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。

十、违约金或者损失赔偿的计算方法

1、甲方逾期付款的，每逾期 1 天，应向乙方支付欠付金额万分之一的滞纳金，但滞纳金累积不超过欠付金额的 5%。

2、乙方逾期提供服务或无故中断服务的，每违约 1 天，应向甲方支付合同总价万分之一的违约金，违约达 30 日，甲方有权解除合同，解除合同的通知自发出之日生效。

3、如乙方不能按本合同约定进行服务的，甲方有权要求乙方在限期内整改。乙方不能在限期内整改或拒绝整改的，甲方有权解除合同，同时要求乙方按照合同总价 5%的标准向甲方支付违约金，解除合同的通知自发出之日生效。

4、一方违反本合同第五条约定的保密义务，守约方有权解除合同，同时违约方应按合同总价的 30%向守约方承担违约责任。如对守约方造成损失，另行计算损失并赔偿。

5、其他未尽事宜，以《中华人民共和国民法典》等有关法律法规规定为准，无相关规定的，双方协商解决。

十一、不可抗力

1、在执行合同期限内，任何一方因不可抗力事件造成不能履行合同时，应立即通知对方，并在 5 日内寄送有关权威机构出具的证明，则合同履行期可延长，延长期与不可抗力影响期相同。出现上述情况不受合同有关违约责任制约。

2、不可抗力影响时间持续 30 日以上时，甲乙双方及时解除合同。

3、本条所述“不可抗力”是指不可预见、不能克服及不能避免的事件，包括战争、严重火灾、洪水、地震等。

十二、争议解决方式

本合同履行过程中发生争议，双方应协商解决或请求调解，否则应提交常州仲裁委员会仲裁；

守约方为解决争议所产生的各项费用（包括但不限于仲裁费、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。

十三、组成本合同的文件包括

1、合同条款；

2、招标文件；

3、乙方的投标文件；

4、甲乙双方商定的其他必要文件。

上述合同文件内容互为补充，如有不明确，由甲方负责解释。

十四、其他

1、如需修改或补充合同内容，应经甲方、乙方协商一致，共同签署书面修改或补充协议。该协议将作为本合同不可分割的一部分。

2、除甲方事先书面同意外，乙方不得转让人和其应履行的合同义务。

3、本合同未尽事宜，按中华人民共和国现行有关法律法规执行。

十五、合同生效

本合同自甲、乙双方授权代表签字并加盖单位公章之日起生效。

十六、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。

（以下无正文）

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

（盖章）

纳税人识别号：

开户名称：

乙方：中国移动通信集团江苏有限公司常州分公司

（盖章）

纳税人识别号：91320400714098134K

开户名称：中国移动通信集团江苏有限公司常州分公司

开户行：	开户行：招商银行北京分行营业部
账号：	账号：8888015100006604
地址：	地址：常州市新北区河海中路 82 号
联系电话：	联系电话：
代表：	代表：
日期：2026年3月30日	日期：2026年3月29日

附件一：网络安全服务内容

按照《GB/T20984-2007》要求，对常州市人力资源和社会保障公共服务与技术保障中心的信息系统资产进行信息安全渗透测试服务，并提供一年的安全服务，服务内容主要包括对互联网资产的渗透测试、安全攻防演练、信息安全咨询、培训服务等。

一、项目内容

（一）总体要求

拟采购的各项服务内容实行流程化管理，服务过程采用规范操作，确保服务质量满足常州市人力资源和社会保障公共服务与技术保障中心信息安全要求；针对常州市人力资源和社会保障公共服务与技术保障中心的实际情况，提供有针对性的安全咨询建议及安全规划和建设方案；及时协助常州市人力资源和社会保障公共服务与技术保障中心信息安全管理人员发现和处理服务范围内的信息安全事件，建立详细的服务管理文档和服务操作文档，确保各项服务活动可追踪、服务效果可验证。

（二）安全服务内容

2.1 网络安全流程规范体系

全面梳理常州市人力资源和社会保障公共服务与技术保障中心网络安全工作机制、职责以及相应流程规范体系：

完善网络安全工作体制机制，明确责任人、责任部门，明确工作职责，发生变化及时更新。制定工作责任清单，协助责任落实。

输出：《网络安全工作职责》《网络安全组织架构图》《网络安全制度》。

2.2 安全检查

针对“市网安”、“省网安”专项行动，在行动开始前，通过安全漏洞扫描、渗透测试、安全配置检查、弱口令检查等方式评估基本网络安全、系统安全、弱口令风险情况等内容。检查结果出具相关报告（包括相关风险及整改建议），并提复测服务，形成安全闭环管理。通过成熟经验，全力保障各应用系统安全、稳定运行。

漏洞扫描：每月进行1 次暴露面机扫，快速发现漏洞，及时整治，确保暴露面资产的安全性。

输出：《漏洞扫描报告》、《漏洞复测报告》。

渗透测试：每季度完成1次渗透测试检查；采用主动防护的手段，每个季度对常州市人力资源和社会保障公共服务与技术保障中心及相关单位相关外网应用系统和网站通过工具和人工检测的方式进行漏洞扫描，查找脆弱性风险，并于每季度最后10日前提交《信息系统安全弱点评估报告及信息安全风险整改方案》。通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法，并配合系统开发商做好漏洞整改、复测工作。

输出：《渗透测试报告》、《渗透复测报告》。

上线评估：对新增API 接口上线前安全评估测试（3天内输出报告）。

输出：《API接口渗透测试报告》、《API接口渗透复测报告》。

安全配置检查：每季度完成1 次配置合规检查。

输出：《安全配置检查报告》、《安全配置加固建议》。

防守报告：基于现有或新增防守设备或平台，在市级网络安全演练中，根据攻击告警日志，输出防守报告。

输出：《防守报告》。

安全通报服务：通过特定方式向采购人提供安全通告列表，实时提供最新出现的安全漏洞和安全升级通告。对于影响力范围广、破坏大的计算机病毒提供具体的检测和修复办法。

输出：《威胁情报》。

2.3网络安全风险防范与处置服务

服务期内由服务方提供安全设备，服务方带安全设备为常州市人力资源和社会保障公共服务与技术保障中心提供网络安全风险防范服务，避免或减少被主管单位的网络安全事件（僵木蠕、APT攻击等事件）通报。另外少量的安全事件通报应支撑甲方及时接收、

处置并反馈市委网信办相关漏洞与网络安全事件通报。

（1）处置前：利用提供的安全设备做好日常的监测、拦截、处置（对内网终端感染僵木蠕、APT攻击等恶意程序，应协助进行处置）。

（2）处置中：根据主管单位下发的恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力等风险事件类型,提出处置方案，并进行处置使之不会再被通报。

（3）处置后：按网信办规范，及时提交处置报告，避免迟报、漏报情况。责任制单位反馈要求。

输出：《日常恶意程序监测记录》《恶意程序处置记录》《XXX通报反馈表》。

2.4 政务信息化项目网络安全管理

为落实《常州市政务信息化项目建设网络安全管理规定》，对新建、改建、扩建政务信息化项目符合网络安全事前审核要求，配合开展相关工作。含以前自然年经审核项目符合事后检查要求。

2.5 网络数据安全管理

1. 针对一个典型系统，落实国家数据分类分级保护制度规定，建立样板，指导其他网络数据准确识别、及时报送重要网络数据目录信息，持续加强数据安全保护。

2.针对上述典型系统，组织开展1次数据安全风险评估。根据《常州市数据安全管理规范指南》指导，从管理和技术层面落实个人信息保护要求。

3.指导督促向境外提供数据的数据处理者依法申报数据出境安全评估、订立个人信息出境标准合同。

4.排查常州市人力资源和社会保障公共服务与技术保障中心违法违规收集使用个人信息专项治理、人脸识别技术应用安全监督检查等。

输出：《XX系统数据安全风险评估报告》、《XX系统分类分级表》、《个人信息出境标准合同》。

2.6 完善保障体系

1.资产梳理：完善网络安全监管平台的资产信息，动态更新维护资产情况。

2..落实政务信息化项目建设网络安全管理相关规定，对政务信息化项目网络安全“三同步”做好自查。

3.按照《互联网政务应用安全管理规定》、《机关事业单位网络身份管理办法（试行）》等要求，落实网络身份管理任务，开展网络身份凭证（电子证书）申领、规范网

上标识加注等工作。

4、落实外包网络安全管理要求，开展外包管理风险排查，强化外包管理，依据《江苏省关于加强党政部门数字化建设中外包活动网络安全管理实施意见》要求，协助开展外包管理。防范因外包人员不当行为引起的重大失泄密案件和网络安全事件。

输出：《外包管理风险排查报告》、《资产梳理表》、《网络安全三同步自查情况》

2.7开展宣传教育培训

培训周期：每年提供一次（安全产品或者信息安全意识方面）提供与常州市人力资源和社会保障公共服务与技术保障中心业务环境密切相关的网络安全教育及意识培训，以提高员工的网络安全防护意识，进一步提高常州市人力资源和社会保障公共服务与技术保障中心网络的安全防护等级和水平。

输出：《网络安全培训课件》。

2.8网络安全周活动支撑服务

2.8.1网络安全攻防实战演练服务

开展网络安全演练活动，帮助安全管理人员、系统工作运维人员、员工提升对网络安全突发事件的发现能力，降低安全事件发生的概率，加强网络安全突发事件发生后的应急响应能力。

输出：《攻防演练实施方案》、《攻防演练总结报告》。

2.8.2安全周活动配合

配合常州市人力资源和社会保障公共服务与技术保障中心完成网络安全活动周相关工作。

2.9 咨询服务

配合常州市人力资源和社会保障公共服务与技术保障中心在网络安全规划与建设、数据安全规划与建设中提供安全咨询服务、产品选型、合理化建议等。数据安全咨询服务：根据中心数据安全信息化发展需求，协助用户做好数据安全网络安全建设的整体规划设计，安全集成项目、数据安全相关事宜的前期方案咨询、中期实施跟踪及后期验收及维护服务。

2.10 其他安全服务内容

配合常州市人力资源和社会保障公共服务与技术保障中心完成市委网信办相关单位考核的相关内容。

附件二：保密协议

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：中国移动通信集团江苏有限公司常州分公司

为加强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网络安全服务项目相关系统数据的安全保密管理，贯彻落实《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》、《中华人民共和国网络安全法》《中华人民共和国密码法》等有关法律法规，确保数据的安全保密，促进数据合法、有效利用，防止发生失泄密事件，防范非法使用行为，本着平等、自愿、协商一致、诚实信用的原则，就乙方为甲方网络安全技术支持服务（下称项目）等工作中的保密事宜达成如下协议。

一、保密信息

（一）在项目中所涉及的项目设计、图片、开发工具、流程图、工程设计图、计算机程序、数据、专利技术、招标文件等内容（在项目中向社会公众提供信息公开和服务的图片、网页、信息数据不包含在内）；

（二）甲方在项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

（三）甲方在项目实施中涉及的业务及技术文档，包括方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据等；

（四）其他甲方合理认为的建议，并告之乙方属于保密的内容。

二、保密范围

（一）甲方已有的技术秘密；

（二）甲方敏感信息和知识产权信息；

（三）乙方持有的科研成果和技术秘密，经双方协商，乙方同意被甲方使用的。

三、保密条款

（一）乙方明确所接收的文件（包括电子和纸质）为甲方所有，甲方拥有以上文件的知识产权。乙方承认甲方在本协议规定的保密信息上的利益和一切有关的权利，乙方

应当考虑甲方的利益对该信息予以妥善保存，防止有意或无意的泄漏；

（二）乙方应采取尽可能的措施对所有来自甲方的信息严格保密，包括执行有效的安全措施和操作规程；

（三）甲方为基础数据的管理和提供方，甲方拥有所有数据的全部所有权，乙方需在甲方的授权下使用数据。乙方承诺对甲方以书面、口头、电子文本、电子数据等方式提供的保密信息承担保密义务；

（四）乙方同意仅在为实施本项目时使用保密信息，绝不为与该项目无关的目的使用保密信息；

（五）未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息和其中的任何部分，披露或透露给任何第三方（仅可向有知悉必要的乙方内部人员披露，同时仅为甲方项目所需使用）。乙方有义务妥善保管上述文件和数据，不得复制、泄漏或遗失。乙方亦不得依据甲方提供的任何保密信息，就任何问题，向任何第三方作出任何建议；

（六）若乙方确有需要向第三方展示甲方数据信息及成果，需提前向甲方以一事一议的形式提交书面申请，由甲方签字盖章同意后方可施行。未经同意，严禁乙方将甲方数据向第三方展示。如有违反，乙方须承担全部后果，甲方有权向乙方追责；

（七）项目维护过程中，如因业务需要，乙方需采购第三方软件或软件服务的。乙方需以数据最小化为原则，明确数据范围及用途，并与第三方签订数据安全保密协议，确保甲方数据安全；

（八）乙方需加强自身保密意识及保密措施，从管理及技术方面保障甲方数据安全，与员工签订保密协议，约束监督员工，防止个别员工将甲方数据泄露；

（九）乙方的职员违背上述承诺，向第三方披露保密信息，或依据该保密信息向第三方作出任何建议，都将被视为乙方违反本协议；

（十）甲方在特定的情况下有收回所提供的文件、数据及其使用的权利；

四、保密信息的所有权

以上所提及的保密信息均为甲方所有。

五、保密期限

（一）本协议的保密期限与主合同一致；

（二）在本协议失效后，如果本协议中包括的某些保密信息并未失去保密性的，本协议仍对这些未失去保密性的信息发生效力，约束双方的行为；

（三）本协议是为防止甲方的保密信息在协议有效期发生泄漏而制定。因任何理由而导致甲、乙双方的合作项目终止时，乙方应归还甲方所有有关信息资料和文件，但并不免除乙方的保密义务。

六、关系限制

本协议不作为双方建立任何合作关系或其他业务关系的依据。

七、违约责任

乙方未遵守本协议的约定泄露或使用了保密信息，甲方有权终止双方的合作项目，乙方应支付甲方主合同总价30%的违约金，并应按甲方的实际损失确定赔偿金额赔偿甲方遭到的其他损失，甲方有权进一步追究其一切相关法律责任。

八、其他事项

（一）本协议未尽事宜，由甲乙双方协商解决；

（二）本协议自甲、乙双方盖章之日起生效。

甲方：（章）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：（章）中国移动通信集团江苏有限公司常州分公司

中国移动通信集团江苏有限公司

附件三：外包网络安全协议

一、协议依据及类型

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_____③_____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

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__%（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

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

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30%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

按照主合同约定的争议解决条款执行。

六、协议期限

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。

七、其他

本协议自甲、乙双方盖章之日起生效。

甲方：（章）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：（章）中国移动通信集团江苏有限公司常州分公司

中国移动通信集团江苏有限公司

防范电信网络诈骗承诺书

为了预防和遏制电信网络诈骗活动，落实《中华人民共和国反电信网络诈骗法》《中华人民共和国刑法》《中华人民共和国网络安全法》《中华人民共和国电信条例》《电话用户真实身份信息登记规定》《关于防范和打击电信网络诈骗犯罪的通告》《工业和信息化部关于进一步防范和打击通讯信息诈骗工作的实施意见》等相关法律法规和文件的要求，我单位(电信用户)订购和使用中国移动提供的电信服务时，承诺严格遵守以下各项要求：

一、我单位申请办理电信业务时，承诺提供真实身份信息。我单位不会为他人实施电信网络诈骗活动提供下列支持或者帮助：(一)出售、提供个人信息；(二)帮助他人通过虚拟货币交易等方式洗钱；(三)其他为电信网络诈骗活动提供支持或者帮助的行为。

二、我单位承诺不会非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等，不会提供实名核验帮助；不会假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

三、我单位承诺会对我单位使用电信服务的行为负责，不会设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不会利用电信网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

四、我单位承诺，如果涉及从中国移动购买物联网卡再将载有物联网卡的设备销售给其他用户的，我单位会核验和登记用户身份信息，并依法将销量、存量及用户实名信息传送给中国移动。

五、我单位承诺不会非法制造、买卖、提供或者使用下列设备、软件：(一)电话卡批量插入设备；(二)具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；(三)批量账号、网络地址自动切换系统，批量接收提供短信验证、语音验证的平台；(四)其他用于实施电信网络诈骗等违法犯罪的设备、软件。

六、我单位承诺依法遵守反电信网络诈骗相关法律法规，主动配合中国移动开展的监督检查与风险排查工作，及时整改发现的问题。

七、如果我单位违反上述规定的，我单位知悉可能面临以下法律责任：

(一)依据《中华人民共和国刑法》，组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，将被依法追究刑事责任，包括但不限于：构成第二百六十六条诈骗罪的，最高可被处十年以上有期徒刑或者无期徒刑，并被处罚金或者没收财产；构成第二百八十七条之二帮助信息网络犯罪活动罪的，最高可被处三年以下有期徒刑或者拘役，并被处或者单处罚金；构成第二百五十三条之一侵犯公民个人信息罪的，最高可被处三年以上七年以下有期徒刑，并被

处罚金；构成第三百一十二条第一款掩饰、隐瞒犯罪所得、犯罪所得收益罪的，最高可被处三年以上七年以下有期徒刑，并被处罚金。

（二）依据《中华人民共和国反电信网络诈骗法》第三十八条、第四十六条，组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一万元的，处十万元以下罚款。从事前款行为的违法犯罪人员，除依法承担刑事责任、行政责任以外，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

（三）依据《中华人民共和国反电信网络诈骗法》第四十四条，非法买卖、出租、出借电话卡等，为他人提供实名核验帮助或假冒他人身份或者虚构代理关系开立电话卡等，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款；没有违法所得或者违法所得不足二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。

（四）其他需要依法承担的法律责任。

八、我单位承诺：如果我单位违反上述规定的，中国移动有权依法依规或者依照电信服务合同约定，停止向我单位提供涉诈电信服务，追究我单位的违约责任。

本承诺书经我单位（或其合法授权代表）签署后生效，构成我单位与中国移动之间电信服务合同（包括各类电信业务协议）的有效组成部分，对我单位具有约束力。

承诺人签署： 徐海

日期： 2026.3.30

中国移动通信集团江苏有限公司

廉 洁 合 作 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：中国移动通信集团江苏有限公司常州分公司

为规范甲、乙双方及其工作人员的廉洁从业行为，保障双方合法权益，预防商业贿赂和不正当竞争，强化廉洁合作监督，防止合作中发生违法违纪违规行为，甲、乙双方在自愿的基础上签署本协议。

第一条 本协议作为主协议的附件，经甲、乙双方签署后生效。一经签订，各方必须严格遵守。

第二条 甲、乙双方应共同遵守下列条款：

（一）严格遵守国家法律法规，坚持廉洁、诚信的原则，恪守商业道德和职业规范。

（二）规范商业合作行为，在履行合同过程中，明确商业行为要求，严格管理双方所属员工，不得从事违反本合同禁止的活动。

第三条 乙方及其员工应遵守下列条款：

（一）乙方工作人员及其配偶、子女、其他特定关系人不得索取、接受或以借用等名义占用甲方或甲方工作人员的财物。

（二）乙方工作人员及其配偶、子女、其他特定关系人不得接受甲方提供的可能影响公正执行公务的礼品、宴请以及旅游、健身、娱乐等活动安排。

（三）乙方工作人员及其配偶、子女、其他特定关系人不得接受甲方提供的礼金和各种有价证券、支付凭证、干股。

（四）乙方工作人员及其配偶、子女、其他特定关系人不得要求甲方支付应由上述人员自行负担的费用或报销票据。

（五）乙方工作人员及其配偶、子女、其他特定关系人不得接受由甲方提供的其他任何可能影响本人公正执行公务的财物或服务。

（六）当甲方提供第三条第（一）至（五）款所指的内容，或实施其他不廉洁行为时，乙方工作人员及其配偶、子女及其他特定关系人应予以拒绝；对于无法拒绝的，应及时向乙方监督部门举报并上缴相关财物。

（七）乙方工作人员在与甲方开展工作过程中，如发现与本人或亲属有利益关系、有可能影响公正履职时，应主动提出回避。

第四条 甲方及其员工应遵守下列条款：

（一）不得给予或以借用等名义向乙方工作人员及其配偶、子女、其他特定关系人提供财物。

（二）不得向乙方工作人员及其配偶、子女、其他特定关系人提供可能影响其公正执行公务的礼品、宴请以及旅游、健身、娱乐等活动安排。

（三）不得向乙方工作人员及其配偶、子女、其他特定关系人提供礼金和各种有价证券、支付凭证、干股。

（四）不得为乙方工作人员及其配偶、子女、其他特定关系人支付应由其本人

承担的费用或报销票据。

（五）不得向乙方工作人员及其配偶、子女、其他特定关系人提供其他任何可能影响其公正执行公务的财物或服务。

（六）乙方工作人员及其配偶、子女、其他特定关系人主动索取和要求本条（一）至（五）款所指的内容，或实施其他不廉洁行为时，甲方应拒绝，并有义务向乙方监督部门及时举报。乙方监督部门应保护甲方当事人的合法权益。

（七）甲方工作人员在与乙方开展工作过程中，如发现与本人或亲属有利益关系、应主动提出回避。

第五条 监督方职责

（一）监督方应当认真履行职责，对本协议的执行情况进行监督检查，接受有关投诉和举报。监督方电话：13906110236、 0519-86816952 。

（二）采取合法手段对甲、乙双方人员遵守法律法规和执行本协议情况开展监督检查。

（三）对项目招标（入围）进行全程监督检查，确保甲、乙双方合法合规、公平公正开展合作。

第六条 违约责任

（一）乙方工作人员违反本协议的，按乙方有关纪律规定处理。

（二）甲方违反本协议（无论是企业行为还是个人行为，都视为甲方违规），乙方有权对甲方收取对应合同金额的1—5%的违约金，并直接从合同应付款中扣除。乙方将视甲方违规情节轻重，分别予以廉政谈话、暂停入围合作、永久终止合作等处理，并根据情况向集团公司采购管理部门、纪检监察部门备案；涉及违法的移交司法机关。

特别提醒：根据最高人民法院、最高人民检察院《关于办理行贿刑事案件具体应用法律若干问题的解释》（法释〔2012〕22号）第一条规定：“为谋取不正当利益，向国家工作人员行贿，数额在一万元以上的，应当依照刑法第三百九十条的规定追究刑事责任”。

（三）甲、乙双方违规当事人今后不得参与对方任何合作业务。

第七条 本协议一式贰份，由甲方、乙方各执一份。

甲方：（签字、盖章）

2026.9.22

乙方：（签字、盖章）

2026 年 9 月 22 日