

洪泽区新一代电子政务外网建设服务



采 购 合 同



甲方：淮安市洪泽区大数据运行维护服务中心（采购人）

乙方：江苏移动信息系统集成有限公司（供应商）

乙方：中国电信股份有限公司淮安分公司（联合体成员供应商）



日 期：二〇二六年一月

政府采购合同协议书

甲方：淮安市洪泽区大数据运行维护服务中心（采购人）

乙方：江苏移动信息系统集成有限公司（供应商）

乙方：中国电信股份有限公司淮安分公司（联合体成员供应商）

甲、乙双方根据项目编号 JSZC-320813-SZZB-G2025-0019 的 洪泽区新一代电子政务外网建设服务 采购项目公开采购结果及采购文件的要求，经协商一致，达成如下合同：

第一条，服务内容及要求

根据《江苏省新一代电子政务外网建设指南》《江苏省新一代电子政务外网固定网络省市对接技术要求》《关于转发全省新“一张网”高质量建设管理有关工作的函》等相关要求，结合我区电子政务外网实际，开展区级新一代电子政务外网建设，以“固移融合”为总体技术路线，以新技术为创新驱动引擎，充分融合 IPv6+、边缘计算、物联感知等信息技术，构建一网多平面、泛在感知、天地一体、高速传输、指挥调度、智能融合、安全可控的新一代电子政务外网。

第二条，合同金额

本合同的总金额（大写）为肆佰捌拾玖万捌仟元人民币。

第三条，服务时间和地点

服务时间：建设期一年，验收合格后，维护、服务期三年。

第四条，付款方式：

1. 合同款分三年（平均）付清（不计利息），每年支付一次。

注：付款时成交供应商须提供正规发票（因发票问题而导致无法正常

付款的，责任由供应商自己承担）。

第五条，验收

验收主体：淮安市洪泽区大数据运行维护服务中心

验收人员：根据采购项目专业性的特点和实际需求，将邀请相关领域专业技术人员不少于3名（含）组成的验收小组，参与验收。

验收时间：服务期一年，以年为验收周期。

验收地点：淮安市洪泽区

验收内容及标准：自合同签订之日起30日内，中标人具备初次交付能力后，并书面向采购人申请初步验收，并按以下要求验收。初步验收合格后，按合同附件3中的《服务考核指标体系》的相关规定进行考核验收。

1. 验收总则

1.1 验收目标：全面验证新一代电子政务外网建设服务是否符合设计规范、合同要求及业务需求，确保网络系统稳定、安全、高效运行，具备支撑各类政务应用的能力。

1.2 验收依据：以项目合同、招投标文件、国家及行业相关标准（如《电子政务外网工程技术规范》）、设计方案及变更文件为核心验收依据。

1.3 验收范围：涵盖网络基础设施（骨干网、城域网、接入网）、网络安全体系（防火墙、入侵检测等）、运维管理平台、数据传输性能及相关服务（如培训、质保）等全环节。

2. 验收人员

2.1 验收小组构成：由采购人（牵头）邀请相关领域专业技术人员不少于3名（含）组成的验收小组，参与验收。

3. 验收核心内容与标准

（一）网络基础设施验收

1. 网络拓扑验收：验证实际网络拓扑是否与设计方案一致，骨干网、城域网、接入网的层级结构及连接方式符合要求，节点覆盖达标。

2. 性能指标验收：通过专业工具测试网络带宽、时延、丢包率、并发连接数等指标，需满足设计标准。

（二）网络安全体系验收

1. 安全设备验收：检查防火墙、入侵防御系统（IPS）、VPN、数据加密设备等是否部署到位，配置是否符合安全策略。

2. 安全防护验收：测试网络边界防护、访问控制、数据传输加密、病毒防护等能力，模拟攻击场景下系统无安全漏洞被利用。

3. 应急响应验收：验证安全事件监测、告警、处置流程的有效性，应急预案可快速启动并恢复系统正常运行。

（三）运维管理平台验收

1. 功能验收：确认平台具备设备监控、故障告警、性能分析、配置管理、日志审计等核心功能，操作便捷、数据准确。

2. 兼容性验收：平台可兼容现有及新增的网络设备、政务应用，数据交互无冲突，支持多终端访问。

（四）服务与培训验收

1. 质保服务验收：核查承建单位提供的服务响应机制（如7×24小时技术支持）是否达标。

4. 验收流程

4.1 申请阶段：承建单位完成自检后，向采购人提交《验收申请表》及全套验收资料。

4.2 资料审核阶段：采购人联合验收小组审核资料，资料合格则启动现场验收；不合格则要求承建单位限期补正。

4.3. 现场测试阶段：验收小组依据验收标准，对网络性能、安全防护、平台功能等进行现场测试，记录测试数据及结果。

4.4. 问题整改阶段：对验收中发现的问题，承建单位需在规定期限内完成整改，并提交整改报告，验收小组复核。

4.5. 结果确认阶段：若所有验收项均达标，验收小组签署《验收合格报告》；若未达标，明确整改期限及重新验收时间。

第六条，履约保证金

乙方应向采购单位交纳中标总价 1%的履约保证金，以保函形式缴纳。

第七条， 侵权处理

乙方应当保证，其依据本合同为甲方提供的技术开发过程中和/或其为甲方提供的技术成果不侵犯任何第三人的合法权益。如果有人提出法律或行政程序（合称“侵权指控”），声称甲方侵犯了其知识产权等合法权益的，乙方应当负责解决，并赔偿甲方就此所承担的一切损失和费用，包括但不限于上述侵权指控中所产生的诉讼费用、合理的律师费用、调查费用、和解金额或生效法律文书中规定的赔偿金额。

第八条，违约责任

1. 双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

2. 乙方未能按本合同约定按期提供技术服务，每逾期 1 日，乙方应当按照本合同费用总额的 1% 向甲方支付违约金。如违约金数额累计达到本合同费用总额的 30% 时，甲方有权终止本合同，乙方仍应支付上述违约金、退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息，同时赔偿甲方的相应损失。

第九条， 合同纠纷处理

本合同执行过程中发生纠纷，由甲乙双方协商解决，若协商不成，作如下 2 处理：

1. 申请仲裁。选定仲裁机构为淮安市仲裁委员会。
2. 提起诉讼。约定由采购人所在地法院管辖。

第十条， 双方约定本合同其他相关事项

1. 任何一方未经另一方同意，不得向任何第三方透露本合同的签订及其内容。甲方向其关联公司透露的，不在此限。

2. 任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同做出的任何修改和补充应为书面形式，由双方签字盖章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时，以补充合同或补充协议为准。

3. 双方约定，乙方在向甲方提供技术成果过程中，根据甲方要求，为甲方指定的人员提供技术指导和培训，并保证培训人员能够熟练操作为止。

第十一条， 组成本合同的文件包括

1. 合同主要条款；
2. 采购文件和乙方的投标文件；

3. 中标通知书;

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,解释顺序以形成时间在后的为准。

甲方(采购人)

单位名称(公章)

法定代表人
或其委托代理人:
(签章)

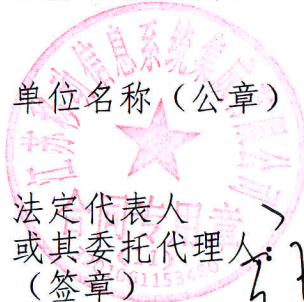


日期: 2026-1-23

乙方(供应商)

单位名称(公章)

法定代表人
或其委托代理人:
(签章)



日期: 2026-1-23

乙方(联合体供应商)

单位名称(公章)

法定代表人
或其委托代理人:
(签章)



日期: 2026-1-23

附件 1

保密协议

甲方：淮安市洪泽区大数据运行维护服务中心（采购人）

乙方：江苏移动信息系统集成有限公司（供应商）

乙方：中国电信股份有限公司淮安分公司（联合体成员供应商）

一、总则

（一）为确保甲乙双方在网络信息安全服务合作事宜有序开展，杜绝信息泄露事件的发生。经甲乙双方友好协商，签订本协议。

（二）本协议适用于的项目名称为：洪泽区新一代电子政务外网建设服务，项目编号：JSZC-320813-SZZB-G2025-0019。

二、信息保密要求

乙方须遵守以下条款，对项目涉及的信息进行保密：

（一）乙方在为甲方提供服务过程中，应对来源于服务对象的所有信息进行涉密情况的征询，对于甲方的保密信息要做好保密管理。

（二）对来源于甲方所有信息（包括但不限于相关技术资料、报告、摘要、纪要、文件、计划、报表、复印件、信息系统应用数据等），乙方负有保密责任，应采取有效保密措施确保信息安全。

（三）乙方人员须在甲方工作人员允许和在场的情况下对甲方内部信息数据进行操作，乙方不得擅自复制、传播甲方的各类信息，不得外泄信息。

（四）乙方在完成相关服务后，将使用的安全技术设备带离现场时，须在甲方监督下及时使用不可恢复的删除方式彻底删除设备内的甲方内部信息。未经甲方许可，不得带走甲方有关文件、资料和数据。

(五) 乙方在提供服务过程中，参与项目的乙方人员应遵守甲方有关规章制度。

(六) 相关服务完成后，乙方应将相关交付物完整交付甲方，不得保留相关交付物的副本，相关纸质及电子资料必须销毁，防止信息外流。

(七) 乙方在工作期间，严格遵守甲方保密制度及有关规定，不得泄露服务对象相关系统及数据库的账号和密码。

(八) 本协议效力不受劳动合同订立及解除的影响，乙方工作人员调离乙方公司时，乙方公司应负责采取相关措施防止信息泄露；否则发生的项目信息泄露责任，由乙方负责。

(九) 乙方与乙方工作人员签订针对本项目的保密协议，确保乙方工作人员严格执行本协议中保密条款。

三、甲方须遵守以下条款，对项目涉及的乙方内部信息进行保密：

(一) 甲方提供涉密技术资料、数据时应向乙方明示。

(二) 甲方不得向任何第三方披露乙方的工作程序，技术工具、设备、方法等。

(三) 甲方不得向任何第三方披露乙方的技术资料或文档，包括但不限于项目过程文档、实施方案等。

四、保密期限

本协议经双方盖章后生效。如果所涉及的保密信息依照国家有关法律法规及其保密期限超过上述规定的年限，则双方的保密责任在这些法律法规规定的年限内继续有效。

五、违约责任：

乙方不得以任何理由、任何形式泄露甲方的相关机密。如果违反，乙方必须承担甲方因此而造成的全部损失（含直接及间接经济损失）；情节严重者，并提请有关部门追究其刑事责任。

【本文结束】

甲方（采购人）

单位名称（公章）



乙方（供应商）

单位名称（公章）



乙方（联合体供应商）

单位名称（公章）



附件 2

网络信息安全承诺书

甲方保证遵守以下各项规定：

第一条，遵守国家有关法律、行政法规和管理规章，严格执行信息安全管理规定。

第二条，不得从事危害国家安全、泄露国家机密等违法犯罪活动，不得利用云服务产品制作、查阅、复制和传播违反《中华人民共和国宪法》和法律、妨碍社会治安、破坏国家统一、破坏民族团结、色情、暴力等的信息，不得利用云服务产品制作、查阅、复制和传播任何含有下列内容之一的信息：煽动抗拒、破坏《中华人民共和国宪法》和法律、行政法规实施的；

1. 煽动颠覆国家政权，推翻社会主义制度的；
2. 危害国家安全，泄露国家机密的；
3. 煽动分裂国家、破坏国家统一的；
4. 煽动民族仇恨、民族歧视，破坏民族团结的；
5. 捏造或者歪曲事实，散布谣言，扰乱社会秩序，破坏社会稳定的；
6. 破坏国家宗教政策，宣扬邪教和封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
7. 公然侮辱他人或者捏造事实诽谤他人，侵害他人合法权益的；
8. 损害国家和/或者国家机关信誉和/或者利益的；
9. 其他违反《中华人民共和国宪法》和法律、行政法规的。

第三条，不得利用本项目服务从事下列危害计算机信息网络安全的活动：

1. 未经允许，进入计算机信息网络或者使用计算机信息网络资源的；
2. 未经允许，对计算机信息网络功能进行删除、修改或者增加的；
3. 故意制作、传播计算机病毒等破坏性程序的；
4. 其他危害计算机信息安全的。

第四条，提供的信息必须遵守国家有关知识产权的法律、行政法规、规



章、政策等规定。

第五条，安装软件及其他作品、数据时，应自行依法具有或取得所需之软件、作品、数据的著作权及使用权许可。

第六条，应妥善保管服务产品的数据，并应对进入和管理服务产品的口令、密码的完整性和保密性负责。自行承担如维护不当或保密不当致使上述数据、口令、密码等丢失或泄漏所引起的损失和后果。

第七条，甲方在收集、存储、传输、处理个人数据时，应做好妥善保管并在法律法规许可的范围内使用。

甲乙双方保证遵守以下各项规定：

第九条，严格遵守《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》《全国人民代表大会常务委员会关于加强网络信息保护的决定》、国务院令 第 292 号《互联网信息服务管理办法》的相关规定，采取技术措施和其他必要措施确保信息安全，在发生或者可能发生信息泄露、毁损、丢失等情况时，立即采取补救措施进行补救。

第十条，甲乙双方在合作过程中，发现存在法律法规明令禁止的情形时，应当立即配合有关部门，停止传输、保存有关记录，并向有关机关或部门报告。

第十一条，甲方提供给乙方的数据、设备等资源，以及甲方业务系统运行过程中收集、产生、存储的数据和文档等资源属甲方所有。乙方应保障甲方对这些资源的访问、利用、支配，未经甲方授权，不得访问、修改、披露、利用、转让、销毁其数据；在服务合同终止时，应按要求做好数据、文档等资源的移交和清除工作。

第十二条，承载甲方数据要参照甲方信息系统进行网络安全管理，乙方应遵守党政信息系统的网络安全政策规定、信息安全等级保护要求、技术标准，落实安全管理和防护措施，接受网络安全主管部门的网络安全监管。

第十三条，甲乙双方合作的服务提供商、数据中心等要设在境内。敏感

信息未经批准不得在境外传输、处理、存储。

第十四条，乙方将采取合理且适当的安全措施，旨在帮助甲方保护甲方的内容免受意外或非法的损失、访问或披露。未经甲方的授权，乙方不会查看、使用、向第三方分发甲方的内容，除非：

1. 为遵守法律或政府机构发布的具有约束力的命令所需。
2. 为维护合法权益而提起的诉讼或仲裁所需。

第十五条，甲方应正确地配置和使用乙方提供的服务，并自行采取一定的安全性措施，对甲方的内容进行保护和备份，包括但不限于使用加密技术、防止甲方的内容被擅自访问，并对甲方的内容进行日常存档。

第十六条，对于由甲方的内容引起的安全漏洞，包括但不限于病毒、特洛伊木马、蠕虫或甲方的内容中包含的其他有害编程惯例，或对于甲方未按本协议约定使用乙方服务而引起的安全漏洞，甲方应承担 responsibility。

【本文结束】

甲方（采购人）

单位名称（公章）



乙方（供应商）

单位名称（公章）



乙方（联合体供应商）

单位名称（公章）



附件 3

本项目考核采用扣分制，总分为 100 分，由甲方根据《服务考核指标体系》进行考核。项目供应商年度考核总扣分不超过 20 分（含 20 分）为合格，不扣减相关费用。

供应商年度考核总扣分超过 20 分以上部分，根据总扣分情况进行处罚：每多扣 1 分，扣减当年合同金额的 2%，扣分累积计算，如年度总扣分超过 40 分（含 40 分），甲方有权终止合同，即视为项目供应商不具备相应的合同履行能力，并向项目供应商索取当年已支付的全部合同款。

甲方有权根据服务考核细则扣除相关款项。

《服务考核指标体系》

指标项	考核内容
1. 工单考核	工单是指由用户发起，经甲方审核确认，交予建设运维单位执行的工作联系单（含电子工单）。甲方定期对工单完成情况进行考核评分。 （1）如未按提交工单规定时间内完成工作，按延误时间扣分。每个工单每延误一个工作日扣 0.5 分，超过 3 个工作日以上（含 3 个工作日）每个工作日扣 1 分，最多扣 5 分。对于非建设运维单位原因造成工单延误的，可根据实际情况不做扣分处理。 （2）所有工单必须按工单要求保质保量完成，如因质量问题造成返工，每个工单扣 0.5 分。 （3）由于运维单位建设或技术服务保障未落实到位，造成用户投诉，运维单位可根据用户的投诉记录进行审核，有效投诉每次扣 0.5 分，造成重大影响的投诉，每次酌情扣 1~2 分。运维单位对用户的有效投诉必须及时作出反馈，并根据投诉内容及时进行整改，不予及时整改将额外扣除 0.5 分/次。
2. 任务考核	任务是指由甲方和建设运维单位双方确认或形成正式记录的各类阶段性工作。所有任务必须按照甲方的要求按时保质保量完成，甲方对此进行考核，未按要求完成的工作每项扣 2 分，超额完成任务酌情适当加分，最多加 1 分。如有特殊原因，书面说明情况并提交采购人认可。 对于非建设运维单位原因造成任务延误，不扣分。
3. 运维考核	运维单位必须建立与项目合同相对应的运维管理体系，如未按要求建立相应的运维管理制度则扣 5 分。运维单位必须严格执行运维管理制度，甲方负责定期对运维管理制度的落实情况进行检查，如发现不符合制度要求的每项扣 0.5

	分。 在运维期内，甲方对运维单位的运维服务质量进行考核，考核范围包括但不限于如下事项： 1. 升级加固 政务系统进行安全加固，对操作系统、Web 服务器、中间件、数据库或其他应用程序升级或安装补丁时，需制定详细的升级实施方案，并报甲方，未完成则按次数计扣分值，1 分/次。升级后政务系统需安全可靠，如有安全漏洞或出现不可访问现象，按事故处理。 政务网络进行升级加固，需制定详细的实施方案，并报甲方，未完成则按次数计扣分值，1 分/次。升级加固后政务网络需安全可靠，如有安全漏洞或出现不可访问现象，按事故处理。 2. 数据备份 日常网络行为重要数据应做备份，如程序文档、数据库数据等，数据不落地可以不备份数据库数据。未做备份的，按发现次数计扣分值，2 分/次。应保证备份程序正常工作，及时监测备份计划，防止出现因磁盘空间不足或程序运行失败造成备份程序无法正常运行，由此造成无备份数据的，按发现次数计扣分值，2 分/次。系统出现数据丢失，需要使用备份数据恢复而无最新备份用于数据恢复时，按次计扣分值，5 分/次。 政务网络中核心路由器、防火墙、交换机、IPS、WAF 等重要网络及安全设备应做配置备份。未做备份的，按发现次数计扣分值，2 分/次。政务网络相关网络、安全设备系统出现故障，需要恢复而无最新备份数据用于恢复时，每次扣 5 分。 3. 培训 培训对象包括建设方和最终用户，培训可以工单形式派发任务，未按时完成任务，按次数计扣分值，2 分/次。 4. 日常监测及巡检 运维单位应对政务网络和政务系统建立相应的日常监测及巡检机制，如用户发现系统不能正常访问的（自身原因的除外），按发现次数计扣分值，1 分/次。 5. 定期工作报告 运维单位应定期提交工作报告，内容包括日常监测、巡检、运维、培训等。运维服务项目工作报告应按每季度、每半年、年终各提交一次，其中每季度提交的工作总结，如未按时提交，按延迟天数计扣分值，0.5 分/天，最多扣 2 分；半年度和年度工作总结，如未按时提交，按延迟天数计扣分值，1 分/天，最多扣 3 分。 一次性建设项目工作总结应于与甲方约定建设完成时间前进行提交，如未按时提交，按延迟天数计扣分值，1 分/天，最多扣 3 分。
4. 用户投诉	由采购人牵头，并派专人负责受理用户投诉，对有效投诉，服务外包单位应尽快落实处理。采购人根据投诉记录对服务外包单位进行评分，有效投诉每次扣 0.5 分，造成重大影响的投诉，每次酌情扣 1~2 分。
5. 事故认定	事故是指由于乙方人为疏忽或设备、系统故障未及时处理所造成的重大事件，故障起始时间以运维单位收到故障消息开始计时。 (1) 访问事故 电子政务网络局部访问中断后(局部中断是指电子政务核心机房到各接入点配置 VLAN 汇聚交换机发生数据通讯故障)，0.5 小时内未响应的、1 小时未到达

	现场处理、设备配置问题 4 小时内未处理完毕、设备导致故障应未及时提供备件支撑超过 8 小时的，每次扣 1 分；以上响应时间内每逾期 1 小时每次扣 1 分；直至通讯恢复正常。 电子政务网络全网访问中断后，0.5 小时内未响应的、1 小时未到达现场处理、设备配置问题 4 小时内未处理完毕、设备导致故障未及时提供备件支撑超过 8 小时的，每次扣 2 分；以上响应时间内每逾期 1 小时每次扣 2 分；直至通讯恢复正常。 (2) 网络安全事故 在政务外网的网络安全服务中，投标人应该主动发现问题，积极帮助甲方整改问题。涉及网络安全事件被上级部门交办后，未及时处理并回复的，每个问题扣 3 分。 (3) 其他 其他事故根据事故造成的影响由考核单位进行评判。事故影响较轻可视情况酌情扣除 0.5~1 分/次；事故影响适中可视情况酌情扣除 3~5 分/次；事故情况恶劣，造成较大损失的，扣除 10 分/次，并由乙方承担相应的损失。
6. 应急响应及处理	当应急突发事件发生时，运维单位应及时配合考核单位处理事件，如因运维单位原因未能及时处理，按延迟天数计扣分值，2 分/天，最多扣 10 分。 当政务网络或政务系统受到攻击，需及时恢复时，如因运维单位原因未能及时恢复系统正常业务，按延迟天数计扣分值，2 分/天，最多扣 10 分。 应急事件处理结果应按考核单位要求及时提交书面报告，如未按时提交，按延迟天数计扣分值，1 分/天，最多扣 5 分。
7. 应急演练	政务网络和信息系统运维单位应建立完善的应急响应预案，在紧急情况下，可以参照预先制定的应急预案进行紧急处理。 定期进行应急演练，确定为二级及以下的政务网络和信息系统应每年进行一次，缺一次扣 5 分。

