常州市政府采购合同

项目名称：常州市应急管理局信息化项目运维管理服务
项目编号：JSZC-320400-JZCG-C2024-0458
甲方：（买方）常州市应急管理局
乙方：（卖方）常州数据科技有限公司

甲、乙双方根据常州市政府采购中心 常州市应急管理局信息化项目运维管理服务项目竞争性磋商的结果，签署本合同。

一、合同内容

1.1 标的名称：常州市应急管理局信息化项目运维管理服务项目

1.2 标的质量：解决采购人信息化项目软件系统运维、软件基础支撑能力、网络安全技术服务和网络线路资源租用等服务，确保常州市应急管理平台正常运转。需执行的国家相关标准、行业标准、地方标准或者其他标准、规范按照现行的国家标准或者行业标准执行。

1.3 标的数量（规模）：

序号	名称
一	**软件系统运维管理**
1	危险化学品安全生产风险监测预警系统运维服务
2	江苏省安全生产行政执法系统（常州）运维服务
3	常州市应急管理局移动应用融合升级、常州市应急管理局应急管理指挥信息系统、常州市应急管理局三年安全生产专项整治信息系统、常州市安全生产许可备案审批“一网通”
二	**软件系统租用和应用服务**
1	舆情监测系统
2	19 枚电子审批签章嵌入平台
3	重点监管企业视频云平台租用（含 100T 视频存储池）
4	云视频点播等服务
三	**网络安全技术服务**
1	云主机虚拟服务器（62 台及以上）系统软件运行维护
2	信息系统网络和信息安全自查服务
四	**网络线路资源租用**
1	市局应急指挥中心（运河路）政务外网（100M）
2	市局应急指挥中心（运河路）互联网（100M）
3	市城运中心企业安全生产监控预警视频云台 MSTP 数字电路（100M）
4	新北区应急管理局与企业安全生产监控预警视频云台 MSTP 数字电路（100M）
5	重点监管企业视频云平台公网出口线路（省、市平台调用，500M）

1.4 履行时间（期限）：运维周期为 12 个月，自本合同生效之日起算。

1.5 履行地点：江苏常州

1.6 履行方式：现场服务加远程支撑

二、合同金额

2.1 本合同金额为（大写）：捌拾捌万贰仟圆（882000元）人民币。

三、技术资料

3.1 乙方应按磋商文件规定的时间向甲方提供与合同标的有关的技术资料。

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、接受本合同标的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 乙方保证所交付的合同标的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、合同款项支付

7.1 分期付款：合同签订后，甲方预付合同金额的 20%；合同金额的 80%待项目实施后，甲方分 4 期（每 3 个月为 1 期，每期为合同金额的 20%）支付给乙方，每期甲方按考核办法对项目实施情况进行考核（考核内容详见附件 1），实际支付金额以每期考核情况与乙方进行结算，直至支付完毕。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。甲方按照上述约定支付款项时，乙方应提前开具 6%增值税普通发票并提供给甲方。

八、税费

8.1 本合同执行中相关的一切税费均由乙方负担。

九、项目考核

9.1 甲方依法组织履约考核工作。

9.2 本次服务项目执行考核管理，考核评分实行百分制，评分标准见附件 1.

9.3 考核等级：考核分为优良、良好、合格、不合格 4 个等级。其中：考核结果 90 分（含 90 分）以上的，为优良；考核结果 80 分（含）-89 分（含），为良好；考核结果 70 分（含）-79（含），为合格；考核结果 70 分以下的，为不合格。

9.4 考核安排：合同生效后，本项目每实施三个月，由甲方组织考核。考核结果于次月 5 日前以书面形式通报。

9.5 考核等级和违约金标准：

1、考核为优良的，全额支付考核服务期内服务费用；

2、考核为良好的，支付考核服务期内服务费用的 80%；

3、考核为合格的，支付考核服务期内服务费用的 60%；

4、考核为不合格的，支付考核服务期内服务费用的 50%。同时甲方有权解除本合同，取消乙方后续服务资格。

9.6 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。考核不合格的项目，甲方依法及时处理。

十、违约责任

10.1 甲方无正当理由拒绝接受乙方提供的合同标的的，甲方向乙方偿付拒绝接

受合同价款总值 5% 的违约金。

10.2 乙方逾期开展服务或无故中断服务或提供的服务不符合合同要求的，经甲方催告后并未整改的，甲方有权提前解除本合同并要求乙方支付合同金额 10%的违约金，违约金不足以弥补甲方损失的，乙方应全额赔偿。

十一、不可抗力事件处理

11.1 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。

11.2 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。

11.3 不可抗力事件延续 45 天以上，双方应通过友好协商，确定是否继续履行合同。

十二、解决争议的方法

12.1 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。守约方为解决纠纷所产生的各项费用（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。

十三、合同生效及其它

13.1 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。

13.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

13.3 本合同正本一式三份，具有同等法律效力，甲方、乙方及财政监管部门各执一份。

甲方：常州市应急管理局

地址：常州市龙城大道 1280 号 1A9

法定代表人或授权代表：

联系电话：

签订日期：2024年 12 月 11 日

乙方：常州数据科技有限公司

地址：常州市关河西路 180 号（恒远大厦四楼）

法定代表人或授权代表：

联系电话：

签订日期：2024年 12 月 11 日

附件 1：

常州市应急管理局信息化项目运维管理服务评分标准

项目名称：		运维单位：		
考核项目	考核内容	计分标准	不合格记录	扣分
服务态度（5）	运维人员言行举止文明礼貌。	一次扣 1 分		
	运维人员遵守合同约定，不得向用户索取小费或加班费等。	一次扣 1 分		
	用户对运维人员服务态度，质量的评价不满意。	一次扣 2 分		
运维服务人员要求（20 分）	运维作业人员应满足采购文件，取得相应的资格证。	一次扣 2 分		
	按投标书配备人员到岗保障；保障人员变更需提前 5 个工作日向市应急管理局报备并审核通过后上岗。	一次扣 5 分		
	运维人员按规定填写记录表并留档。	一次扣 2 分		
	运维人员根据运维合同约定的频次、内容、要求进行检查，并出具书面资料。	一次扣 5 分		
	运维单位服务过程中发现的问题应及时处理，不能及时处理的应制定相应的整改方案，并在记录表中形成闭环。	一次扣 2 分		
	运维人员未主动向服务项目反馈运维情况，并由服务项目人员签字确认。	一次扣 2 分		
	运维记录、表格记录应在服务项目留存一份备案。	一次扣 2 分		
运维服务事项要求（20 分）	运维单位设 24 小时应急值班电话，电话无人接听每次扣 3 分。	一次扣 3 分		
	熟练掌握装备与融合通信系统的互联互通技术、应急指挥系统、熟练使用应急指挥设备。	一次扣 2 分		
	每周对各云服务器进行巡查，及时向市应急管理局反馈系统应用异常情况，提交系统巡查报告。	一次扣 2 分		
	按照采购需求，加强软件系统运维管理，开展应用培训指导、基础数据更新、预警信息发布、数据分析审核、应用通报考评，组织相关技术人员对常州市应急管理信息系统加强数据规范管理，研究功能提升并提交系统功能优化建议方案。	一次扣 5 分		

网格安全（50 分）	未如实承诺，合同签订之日前三年及服务期内，存在违反网络安全、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，被公安、网信等部门文件通报至市应急管理局。	一次 50 分		
	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。	一次 50 分		
	运维单位未主动签订或督促外协单位签订《外包网络安全协议要点》《信息安全保密协议》，明确双方权利和义务。	一次扣 10 分		
	运维人员应保守信息安全保密协议，被发现存在违反网络安全、数据安全和个人信息保护等规定行为。	一次扣 5 分		
	被公安、网信部门通报，运维管理服务范围内资产存在高危漏洞。	一个扣 2 份		
应急处理（5 分）	接到日常故障报修后，运维人员必须在合同约定时间内赶到现场处理。	每超时 2 小时扣 1 分		
	一般故障应在 48 小时内处理完毕；特殊情况，需双方确认处理方案除外。	每超时 6 小时扣 2 分		
得分				

附件 2：

保密及网络安全协议

甲方：常州市应急管理局
通讯地址：常州市龙城大道 1280 号 1A9
联系方式：0519-85683167
乙方：常州数据科技有限公司
通讯地址：常州市关河西路 180 号（恒远大厦四楼）
联系方式：0519-83600231

鉴于：常州市应急管理局信息化项目运维管理服务(JSZC-320400-JZCG-C2024-0458)项目（以下简称“项目”），甲方与乙方进行技术及业务合作事宜，双方将以书面或口头形式要求对方提供拥有或已经拥有的对方某些非公开的、保密的、专业的信息和数据，避免因信息泄露而给合作双方造成损失。同时，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要求，为保护甲乙双方及项目参与人员的合法利益，保证合作双方实现顺利合作，参与本项目的所有公司员工应承诺遵守本保密及网络安全协议。为此，双方达成协议如下：

第一条 定义

1. 保密信息指披露方以口头告知、以磁盘或电子形式或书面方式标注或指定为保密信息的非公开信息，以及根据披露时的客观情况应当被视为保密信息的非公开信息。披露方将以直接或间接的方式向接收方披露其技术信息、财务数据、商业合作、数据信息等。这些信息在披露时以口头告知、以磁盘或电子形式或书面标示为“保密”的。保密信息包括且不限于：

（1） 有关合作或交易活动本身相关的一切活动及相关信息（含任何接触、磋商、讨论、开会、谈判、调查、签署文件等相关活动相关的各种信息），包括历史的、现在的和即将发生的；

（2）经营信息，其范围主要包括股东、投资人及关联方信息、公司决议、公司组织架构、股权架构、重大投资交易、成本与收益分析、行业竞争优劣势分析、客户与供应商资料、营销计划、商业模式、市场拓展筹备计划、合同内容、投标中的标底与标书内容、采购资料、定价策略、进货渠道、产品策略、财务报表及财会档案、工资福利分配方案、人力资源信息、法律纠纷等等；

（3）项目信息，其范围主要包括项目货值明细、规划条件和数据、设计文件和数据、土地使用权划拨、出让或出租合同及其相关信息、各类工程图纸、模型、平面图和示意图、建设工程量、工程节点和相关数据、税务信息、计算依据和凭证、项目人员配置和人员信息、不动产权证及其他项目证照和备案文件、房产原值和评估信息、项目财务信息和会计账簿及数据汇总表、租赁合同及其相关租赁信息等等；

（4）技术信息，其范围主要包括知识产权、技术方案、信息系统设计方案、操作流程、制造方法、技术指标、技术文档、计算机软件、计算机程序、数据库、图纸、样品、样机、模具、操作手册、涉及保密信息的业务函电等等；

（5）数据信息，其范围主要包括披露方提供的数据、程序、用户名、口令和资料，以及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。

（6） 属于第三人或第三方的保密信息但依照法律规定或者有关约定，甲方承诺对外承担保密义务的信息；

（7）专项保密信息：甲方和乙方进行的特定合作项目中由甲方披露以及项目涉及的一切信息；

（8） 甲方以书面方式在披露时标注“保密”的信息；

（9）任何甲方未予公开的其他商业信息，或其他甲方合理认为，并告知乙方属于保密的内容。

2. 保密信息范围包括以下信息：

（1）甲方已有的技术秘密；

（2）甲方敏感信息、内部管理信息、经营管理信息、业务信息、知识产权信息；

（3）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。

3. 保密信息范围不包括以下信息：

（1）在接受保密信息之时，乙方已经通过其他来源获悉无保密限制的信息；

（2）一方通过合法行为获悉已经或即将公之于众的信息；

（3）根据政府要求、命令和司法条例所披露的信息。

4. 网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

第二条 甲方权利义务

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，甲方有权单方终止项目合同，且仅支付乙方相应服务期限内合理费用的 10%；乙方应及时返还多收取的价款：

（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的，乙方应主动告知甲方该情况，甲方经评估后，确认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，甲方有权单方终止项目合同，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。

第三条 乙方权利义务

1. 乙方承诺遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》及有关法律法规和行政规章制度、文件规定。

2. 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。

3. 乙方应按照相关规定，进一步加强网络与信息安全的监督管理，严格落实信息安全突发事件“每日零报告制度”，对本单位出现信息安全事件隐瞒不报、谎报或拖延不报的，要按照有关规定，给予责任人行政处理；出现重大信息安全事件，造成重大损失和影响的，要依法追究有关单位和人员的责任。

4. 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，包括执行有效的安全措施和操作规程，不得对外提供、公开、泄露或利用。

5. 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。

6. 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。

7. 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。

8. 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。

9. 乙方应完善数据安全防护，制定应急预案，切实加强数据收集、存储、使用、加工、传输、提供、公开、销毁等全流程各环节安全管理，协助相关部门处理系统漏洞、病毒、网络攻击、网络入侵等安全风险。

10. 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。

11. 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。

12. 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。

13. 乙方承诺未经书面同意，不得直接或间接以任何形式或任何方式把保密信息或其中的任何部分，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）以及提供可以接触上述保密信息的手段，包括在公开场合展览，公开对外宣传，作为文章、讯息、参考数据发表；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。

14. 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，在对数据安全的要求未实施适当的控制之前乙方不应向第三方以　及外包服务提供权限进行数据的访问。

15. 乙方仅可为双方合作之必须，将保密信息披露给其指定的第三方公司，乙方需与第三方公司签订保密协议，第三方公司需以书面形式承诺保守该保密信息。

16. 乙方仅可为双方合作业务之必需，将保密信息披露给其直接或间接参与合作事项的管理人员、职员、顾问和其他雇员（统称“有关人员”），但应保证该类有关人员对保密信息严格保密。乙方需与有关人员签订保密协议。

17. 乙方承诺和保证，除第一条第 3 款或甲方主体不存在，将一直对甲方披露的保密信息进行保密。

18. 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，对其员工进行必要的数据安全意识、技能培训和教育，使其满足工作

要求，并与员工签订保密协议，约束监督员工，防止个别工作人员将甲方数据泄露。员工离岗或授权期满后应当按要求及时做好数据、文档、权限等资源移交收回工作。

19. 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。

20. 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。

21. 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。

22. 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。

23. 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。

24. 项目完工初验时，乙方应向甲方移交系统、数据库、服务器等核心设备超级管理权限、账号、密码。乙方应配合甲方做好管理员、审计员和安全员岗位的培训工作并留下操作手册、培训文档。乙方提供的竣工资料应尽量详尽，包含但不限于移交清单、竣工图纸、技术方案、项目试运行报告、项目测试报告、项目操作手册、项目测试报告、质量保证书、培训计划等。

25. 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。

26. 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。

27. 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。

28. 若乙方在本条中所述的第三方公司或本条中所述的有关人员违反本协议的保密义务，乙方须承担相应责任，并赔偿甲方由此造成的损失。

第四条 违约责任

1. 乙方未遵守本协议的约定泄露或带着与该项目无关的目的使用了本协议约定的保密信息，甲方有权终止双方的合作项目，并有权要求乙方承担由此给甲方造成的全部损失，损失无法确认的，至少承担合作项目金额 10%的违约金。甲方有权保留进一步追究其一切相关法律责任的权利。

2. 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 20%或人民币 10 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。

第五条 没有得到甲方的书面同意，乙方不得将其在本协议书项下的权利

和义务转让给第三方。

第六条 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。

第七条 双方同意，本协议生效后，如国家颁布有关的法律法规与管理条例，双方有义务遵守这些法律法规与管理条例。

第八条 本协议的各部分构成完整的保密及网络安全协议，并取代双方此前任何有关本协议所述事项的理解或协议。未经他方书面同意，本协议不得变更或修改。

第九条 双方承认并同意，除甲方以书面形式明确表达外，甲方向乙方披露保密信息并不构成甲方向乙方转让或授予乙方享有甲方对其数据、技术秘密或其他知识产权拥有的利益。

第十条 本协议接受中国法律管辖并按中国法律解释。对因本协议项下各方的权利和义务而发生的有关的任何争议，双方应首先协商解决，如无法通过协商解决，则应在甲方所在地人民法院诉讼解决。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。

第十一条 双方约定的通讯地址以本协议载明的通讯地址为准。若有变更需及时书面通知对方，一方向另一方寄送的文件或资料如被退回或拒收的，自被退回或拒收之日起即视为送达。本协议载明的通讯地址同时适用于诉讼或者仲裁程序的各个程序中的法律文书的送达。

第十二条 双方约定双方签订的其他合同、协议发生部分或全部无效、终止、解除等情形的，不影响本协议的效力。

第十三条 本协议自双方签字盖章之日起生效，与项目合同起止期限相同，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。项目结束后，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。

第十四条 本协议是为防止甲方的保密信息在双方合作期间发生泄漏以及维护双方合作过程中的网络安全而制定。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和网络安全责任。

第十五条 本协议一式叁份，甲方、乙方及财政监管部门各执一份，具有同等法律效力。

甲方：常州市应急管理局

授权代表：

签订日期：2024.12.11

乙方：常州数据科技有限公司

授权代表：

签订日期：2024年12月11日