

(合同编号: JSZC-321300-JZCG-G2024-0074)

政府采购合同

(服务)

项目名称: 市级政务云统一安全服务项目

项目编号: JSZC-321300-JZCG-G2024-0074

甲方1 (全称): 宿迁市大数据中心

甲方2 (全称): 宿迁市楚润数据集团有限公司

乙方 (全称): 京东科技信息技术有限公司



甲方1（全称）：宿迁市大数据中心（采购人）

甲方2（全称）：宿迁市楚润数据集团有限公司（采购人）

乙方（全称）：京东科技信息技术有限公司（供应商）

依据《中华人民共和国民法典》、《中华人民共和国政府采购法》等有关法律法规，以及本采购项目采购文件（征集文件）、乙方的《投标（响应）文件》及《中标（成交）通知书》，甲乙双方同意签订本合同。具体情况及要求如下：

一、合同内容

（一）标的名称：市级政务云统一安全服务项目

（二）标的质量：符合采购文件要求，乙方完全响应采购文件要求。

（三）标的数量（规模）：详见合同清单。

（四）履行时间（期限）：1年。

（五）履行地点：宿迁市。

（六）下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。

如果下文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合的多个文件的优先适用顺序如下：

1.1 合同组成部分

1.1.1 本合同及其补充合同、变更协议；

1.1.2 成交通知书；

1.1.3 响应文件(含澄清或者说明文件)；

1.1.4 磋商文件(含澄清或者修改文件)；

1.1.5 其他相关采购文件。

二、合同金额

（一）本合同总价为：¥2900000元（大写人民币：贰佰玖拾万元整）。

总价（不含税）为：¥2735849.06元（大写人民币：贰佰柒拾叁万伍仟捌佰肆拾玖元零陆分）。

税款为：¥164150.94元（大写人民币：壹拾陆万肆仟壹佰伍拾元玖角肆分）。

税率为：6%。

（二）合同清单



序号	服务名称	单位	数量	单价	总价
(一) 互联网区域					
1	Web 应用防火墙 (云 WAF)	实例/年	1	¥34,560	¥34,560
2	带宽扩展包	个/年	25	¥3,000	¥75,000
3	域名扩展包	个/年	50	¥4,000	¥200,000
4	Web 应用防火墙 (负载均衡服务型)	实例/年	30	¥5,910	¥177,300
5	主机安全	资产/年	860	¥400	¥344,000
6	网站威胁扫描	实例/年	1	¥3,600	¥3,600
7	实例扩展包	个/年	59	¥705	¥41,595
8	堡垒机	实例/年	1	¥22,810	¥22,810
9	云解析 DNS	实例/年	9	¥320	¥2,880
10	云防火墙	实例/年	2	¥41,400	¥82,800
11	移动安全检测服务	次/年	4	¥8,000	¥32,000
12	安全事件处置系统	套/年	1	¥6,000	¥6,000
13	安全运营中心	资产/年	860	¥400	¥344,000
14	数据库审计	实例/年	1	¥12,960	¥12,960
(二) 电子政务外网区					
1	安全应用网关	套/年	1	¥36,000	¥36,000
2	堡垒机	实例/年	1	¥22,810	¥22,810
3	数据库审计 (电子政务外网)	实例/年	1	¥21,600	¥21,600
4	主机安全	套/年	1	¥220,000	¥220,000
5	本地 DNS 解析服务	套/年	1	¥8,085	¥8,085
6	安全运营中心	套/年	1	¥238,000	¥238,000
7	密码服务平台	套/年	1	¥216,000	¥216,000
8	网站威胁扫描	套/年	1	¥38,000	¥38,000
(三) 安全运营托管服务					
1	安全运营托管服务驻场人员	人/年	4	¥180,000	¥720,000
投标总报价(人民币:元)					¥2,900,000

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, 技术资料的具体形式由甲方指定 (电子或者纸质等)。

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，同时视为乙方违约。

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、合同款项支付及工期

工期：服务期1年。

预付款：乙方自愿降低预付款比例。合同签订后，驻场服务团队需在3天内进场且甲方2在收到乙方发票和相关付款申请材料后10个工作日内，支付70万作为预付款；

进度款：服务时长满2个月经甲方确认后，甲方2在收到乙方发票和相关付款申请材料后10个工作日内，向乙方支付至合同价款的50%；服务期结束并经甲方确认且验收合格，在收到乙方发票和相关付款申请材料后10个工作日内付清余款（无息）。

资金支付的主体：宿迁市楚润数据集团有限公司；

乙方收款账户

乙方开户银行：中国建设银行北京经济技术开发区支行。

乙方开户名称：京东科技信息技术有限公司。

乙方开户账号：11050171360000000514。

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、服务标准

10.1 乙方所提供云网安全服务须符合国家和省网络和数据安全相关规定以及《宿迁



市政务云管理暂行办法》。

10.2 乙方所提供云网安全服务须支持实时监测、弹性调整。

10.3 云网安全服务需满足信息系统安全合规需求（信创改造除外），安全防护包应提供攻击检测与防御、主机监控、运维审计、数据库审计、漏洞扫描、安全应用网关、主机病毒防护、安全态势感知等。

10.4 本项目的总金额包括：宿迁市市级政务云（互联网区域和电子政务外网区域）及电子政务外网网络和数据安全驻场服务、安全运营等服务费用等。

10.5 本项目需求清单中“（一）互联网区域”和“（二）电子政务外网区”安全边界范围为宿迁市政务云上的主机安全和边界安全，不涉及上云业务系统软件自身安全（主要指业务逻辑、系统版本、中间件等）。

十一、项目实施方案要求

11.1 政务云安全现状分析要求

乙方须对宿迁市市级政务云安全现状进行全面分析，包括基础设施安全、云安全、数据安全、安全运营等方面，综合评价安全现状，识别安全问题和主要风险，并提出初步整改建议，要求分析完全贴合宿迁市市级政务云安全实际情况，甲方需要时，乙方应提交相应的报告。

11.2 电子政务外网安全现状分析要求

乙方须对宿迁市电子政务外网骨干网系统安全现状进行全面分析，包括物理环境安全、通信网络安全、区域边界安全、计算环境安全、安全管理中心、安全运营等方面，综合评价安全现状，识别安全问题和主要风险，并提出初步整改建议，要求分析完全贴合宿迁市电子政务外网骨干网系统安全实际情况，甲方需要时，乙方应提交相应的报告。

11.3 政务云安全建设要求

乙方须基于宿迁市市级政务云安全现状，以安全产品和服务能力为基础，以等保合规为基准，构建宿迁市市级政务云纵深防御、主动防御、动态防御、精准防御、统一运营的多维立体安全防护体系和混合多云统一安全运营体系。

11.4 政务云商用密码安全改造要求

乙方须基于宿迁市市级政务云商用密码安全现状，以安全合规的商用密码产品为基础，构建“统一规划、功能全面、稳定可靠、集约高效”的政务云商用密码基础设施，打造服务能力全面、运营一体高效、安全自主可靠的宿迁市市级政务云商用密码安全体



系，夯实密码应用服务核心基础，可便捷高效地向上云系统提供相关增值服务。商用密码基础设施在交付使用前，乙方应按规定将相关方案报主管部门审核。

11.5 安全运营服务要求

11.5.1 安全运营人员

提供不少于 4 名驻场安全运营工程师，驻场地点为宿迁市，具体地点由甲方 1 指定。提供日常 5 天×8 小时现场驻守服务，7 天×24 小时在线响应支持服务，具体负责宿迁市市级政务云网的日常安全运营的各项服务。按月、季度、半年、年时间段形成相关安全形势分析报告，及时向甲方 1 报告。

11.5.2 安全对接服务

响应对接安全主管部门、资源管理岗、运维管理岗交办的安全任务和事件工单，组织评审制定安全响应方案，上报安全任务和安全事件的完成情况，负责对识别收集到的安全事件、安全动态及时预警上报。

11.5.3 日常巡检服务

日常实时监控政务云及电子政务外网边界、云平台及云上系统的安全风险、安全告警，及时上报和处理云上安全事件，定期分批对云上系统进行渗透漏扫，定期产出巡检报告、漏扫报告和处置建议。

11.5.4 安全加固服务

依托相关管理工具，跟踪推进云上安全漏洞的修复与加固，对完成修复加固的系统进行回归性渗透漏扫，产出漏洞关闭报告。

11.5.5 配置实施服务

本项目涉及各安全产品或设备安全配置和管理工作，须登记日常配置实施记录，归档安全产品相关配置备份。

11.5.6 安全内控服务

收集识别业界安全相关动态、事件、政策等，开展内部安全宣贯和改进，负责内部安全相关技术评审和指导，协助运维管理岗监督安全保密制度的执行落实。

11.5.7 应急响应服务

响应安全突发事件和安全应急演练工作，按照流程和预案，分工协作完成事件处置和演练，产出事件处置报告和演练报告。

11.5.8 安全评估服务



对上云系统上线前开展安全评估，产出安全评估报告，配合云上系统等保测评，提供云安全保障方面的咨询和佐证资料。

11.5.9 规范修订服务

识别并登记安全保障过程中上云部门、系统厂商等提出的意见、建议、问题等，提炼共性特征，为运维相关流程制度和应急预案的持续改进，提供修订依据。

11.5.10 重大活动保障服务

在每年护网行动、两会、重大国际国内活动和重要节假日等重要时期，提供安全保障，为客户提供重大活动安全运维服务。

十二、售后服务要求

12.1 乙方需提供完备的运维服务方案，包括运维服务承诺，服务体系、服务措施、响应时间、运维维护方式。

12.2 乙方需提供 7×24 小时在线响应支持服务，乙方应根据甲方业务需要配备本地驻场服务团队，并配不少于 4 人的驻场服务人员。驻场服务人员要求熟练掌握云平台架构，能及时发现并处理网络及云平台常见性故障。

12.3 在信息系统出现重大异常或其他紧急情况，对宿迁市级政务云网总体运行产生影响的，立即向运行管理单位报告，及时断开网络连接并妥善处置，将相关影响减至最小。同时应在断开网络连接后 30 分钟内，将相关情况告知使用单位。在服务期内，应提供驻场服务，对紧急程度高的故障须在 1 小时内解决并恢复，对紧急程度中的故障须在 2 小时解决并恢复，对紧急程度低的故障须在 4 小时解决并恢复。

12.4 服务团队人员应明确各工作岗位的设定和责任边界，上岗应取得甲方同意，不得随意减配人员数量，降低人员素质要求。

12.5 配合宿迁市大数据中心进行宿迁市级政务云网应急预案日常演练和实战流程。

12.6 乙方需列出项目培训方案的详细计划，包括培训内容、时间、地点、人次，重点对相应应用的操作、使用供应商须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由乙方负责，甲方不承担责任。

12.7 乙方须遵循网络安全、数据安全相关标准，采用信息安全技术，建立包含管理安全和技术安全的安全保障体系。

十三、安全审查和保密要求



宿迁市市级政务云网是政府重要的财产信息，涉及个人隐私和商业秘密，关系群众和企业的重大利益，因此，在项目实施中要做好信息安全保护工作。

（一）技术情报和资料的保密要求

1. 接受方应对其从披露方处获知、收到的所有保密信息予以严格保密，确保保密信息不被本协议以外的其他方直接或间接接触、获悉；

2. 任何一方不得将保密信息用于除合作事项以外的其他目的，也不得将保密信息再披露给本协议以外的其他方；

3. 除为进行合作事项所必需以外，不得复制或部分复制披露方提供的保密信息，或以其他方式制作副本、备份等；

4. 除为内部留底并经披露方确认以外，在披露方根据主合同的约定提出合理请求或合作事项终止后，根据披露方的要求，向披露方返还相关保密信息的所有书面及电子形式的文件、记录、资料（包括其副本和复制品），或者销毁上述文件、记录、资料。

乙方有责任维护甲方提供的的数据资料所有权和保密性，不得向第三方提供甲方的数据资料，不得将甲方提供的的数据资料用于本合同以外的用途。若发现，甲方有权要求乙方赔偿由此造成的直接损失，并根据国家有关保密规定追究责任。

（二）等保合规安全性要求

按照《中华人民共和国密码法》及《网络安全等级保护条例》规定，开展等级保护建设工作，本项目要满足国家、省、市等级保护管理有关法律法规和标准规范要求，满足等级保护三级要求，并配合宿迁市大数据中心完成等保测评相关工作。

（三）密码应用安全性要求

按照《中华人民共和国网络安全法》及国家《商用密码管理条例》规定，逐步开展商用密码应用改造相关工作，建设密码服务平台，满足国家、省、市密码管理有关法律法规和标准规范要求，并配合宿迁市大数据中心完成密评测评相关工作。

十四、考核评价要求

1、乙方应设计科学的服务团队内部考核规范，根据日常服务行为进行考评打分。不满足甲方要求的人员应及时更换。

2、甲方会同政务云服务单位、政务云使用单位等制定宿迁市大数据中心云服务安全考核制度，依据全年考核结果支付服务费用。

3、根据宿迁市政务云安全运营考核细则，按年开展安全服务商服务质量考核，提



升精细化管理水平。合同期满，甲方根据考核情况进行扣款。服务考核满分 100 分。

服务质量考核评价扣除费用：

- 1) 考核评价得分 \geq 90 分，不扣费用；
- 2) 90 分 $>$ 考核评价得分 \geq 60 分，扣除合同总价款的(100-得分)%；
- 3) 60 分 $>$ 考核评价得分，扣除合同总价款的 50%；

宿迁市政务云安全运营考核细则如下：

服务类别		打分细则（符合甲方规范要求，包括但不限于）	扣分标准
1、基础服务 (45 分)	1、制度执行（10 分）	1、乙方应依据国家、省相关网络安全法规执行。	每出现一次不符合扣 2 分，扣完为止
		2、乙方应服从甲方的管理制度。	每出现一次不配合扣 2 分，扣完为止
		3、乙方应协助甲方编制或优化政务云安全制度。	每出现一次不配合扣 2 分，扣完为止
	2、运维服务（10 分）	1、乙方应为甲方提供重要会议或重大活动期间的服务	重保期每出现一次事故扣 1-3 分，扣完为止
		2、乙方应按周、月、季、年出具安全运营报告，统计分析政务云运行情况，提出优化意见和建议	每出现一次遗漏扣 1 分，扣完为止
	3、人员服务（15 分）	1、提供不低于 4 人的驻场运维服务。	经甲方检查发现一次不符合，扣 2 分，扣完为止
		2、乙方应建立健全内部管理制度，加强政务云相关人员管理、岗位培训和安全保密教育工作	经甲方检查发现一次不符合，扣 2 分，扣完为止



		3、乙方不得利用工作之便窥探、复制、传播政务云数据，不得泄露、盗取市大数据中心及用户平台、系统和网站账号、密码和内容，转发或传播给其他人员	每发生一次按情况严重程度扣 1-5分，扣完为止
		4、乙方应建立值班制度，向甲方提供驻场人员值班表和值班电话，人员变动须经甲方书面批准	每出现一次按情况严重程度扣 1-3分，扣完为止
		5、乙方应提供良好的服务态度，不得恶意骚扰、辱骂、欺骗、讥讽、威胁、中伤客户等，不得拒不配合市大数据中心做好云使用单位沟通和协调工作的	每发生一次按情况严重程度扣 1-3分，扣完为止
	常规安全（10分）	1、乙方需做好网络安全合规工作，并配合甲方做好安全工作和安全培训。	每出现一次整改不满足要求或不配合，按影响程度，扣 1-3 分，扣完为止，扣完为止。
2、安全服务（55分）	1、安全会商（10分）	1、配合甲方做好申请单位的上云安全会商、评估上云安全防护方案和安全风险，参与会商并给出专业意见。	每出现一次上云安全评估不配合或评估不准确，根据情况影响程度扣 1-3分，扣完为止



2、资源开通和变更 (10分)	1、甲方提出安全防护资源开通和变更需求，乙方须根据甲方需求提供及时服务。	每出现一次资源开通或变更不配合或不及时，根据情况影响程度扣 1-2分，扣完为止
3、安全风险预警 (10)	1、配合甲方做好云上单位安全风险监测和通报，做好安全风险预警工作。	每出现一次安全风险预警不及时或不通报，根据情况影响程度扣 1-2分，扣完为止
4、安全应急处置 (10)	1、配合甲方协助云上单位做好安全事件的应急处置，不得拒绝、消极处置安全事件。	每出现一次应急处置不配合或不积极，根据情况影响程度扣 1-3分，扣完为止
5、材料归档 (5分)	1、配合甲方做好政务云安全服务相关材料的归档。	每出现一次不配合或不及时，根据情况影响程度扣 1-5分，扣完为止。
6、通报扣分(5分)	1、被上级有关机构检查通报安全问题，对通报情况进行扣分。	若因乙方工作不尽职原因造成甲方被通报批评，每发生一次扣 5分。
7、红线行为 (5分)	1、违反市大数据中心管理规范，拒不接受相关处理，给市大数据中心内部管理、声誉或利益造成严重损害的行为	每出现一次按情况严重程度扣 1-3分



		<p>3、在我市政务云服务过程中，由于服务态度、过度承诺、工作疏忽等，引起客户投诉，或给市大数据中心或客户造成重大影响（重大影响指行为后果给市大数据中心或客户造成实际经济损失，或对市大数据中心的公众形象带来负面影响等）</p> <p>4、未将客户处发生网络安全事故及时上报市大数据中心，给客户带来不良影响和损失的</p> <p>5、由于自身技术原因或服务管理原因造成的人为事故，引起客户有效投诉，对市大数据中心带来不良影响的</p> <p>6、对客户的询问不予说明清楚、含糊其辞，引起用户单位误解的</p>	
5、加分项	1、服务情况	<p>1、对政务云安全服务满意，使用单位对甲方书面感谢的，每次加 1 分</p> <p>2、协助甲方获取市级及以上书面肯定，每次加 3-5 分</p>	
	2、优化改进	<p>在日常工作中能主动思考，提出合理化举措建议并被甲方采纳的，每次加 1 分</p>	



十五、项目验收

合同签订后 2 个月内，乙方按照合同服务清单提供对应安全产品及服务，项目服务期结束后，甲方根据服务情况，3 个工作日内组织验收并出具加盖甲方公章的验收报告。

15.1 甲方依法组织履约验收工作。

15.2 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。

15.3 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。

15.4 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。

15.5 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条件挂钩。履约验收的各项资料存档备查。

15.6 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《中华人民共和国民法典》。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。

十六、违约责任

16.1 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 1‰ 的违约金。

16.2 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 1‰ 每日向乙方支付违约金。

16.3 乙方逾期交付合同标的的，乙方应按逾期交付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 个工作日不能交付合同标的的，甲方可解除本合同。乙方因逾期交付合同标的的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 1‰ 的违约金

16.4 乙方交付合同标的的标准不符合合同规定及磋商文件规定标准的，甲方有权



拒绝接受合同标的，并可单方面解除合同。

十七、乙方合法权益补偿机制

乙方合法权益补偿救济机制。在履约过程因政策变化、规划调整而无法履行合同约定，造成企业合法权益受损的，甲方依据实际情况对乙方进行补偿救济。

十八、不可抗力事件处理

18.1 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。

18.2 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。

18.3 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。

十九、解决争议的方法

19.1 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。

二十、合同生效及其它

20.1 合同经三方法定代表人或授权委托代理人签字并加盖单位公章后生效。

20.2 本合同未尽事宜，遵照《中华人民共和国民法典》、《中华人民共和国政府采购法》有关条文执行。

20.3 本合同正本一式陆份，具有同等法律效力。

20.4 附件：数据安全保密协议和网络与信息安全责任条款。

(以下无正文)

甲方1：宿迁市大数据中心

法定代表人或授权代表（签字）：

联系人：

电话：

甲方2：宿迁市楚润数据集团有限公司

法定代表人或授权代表（签字）：

联系人：



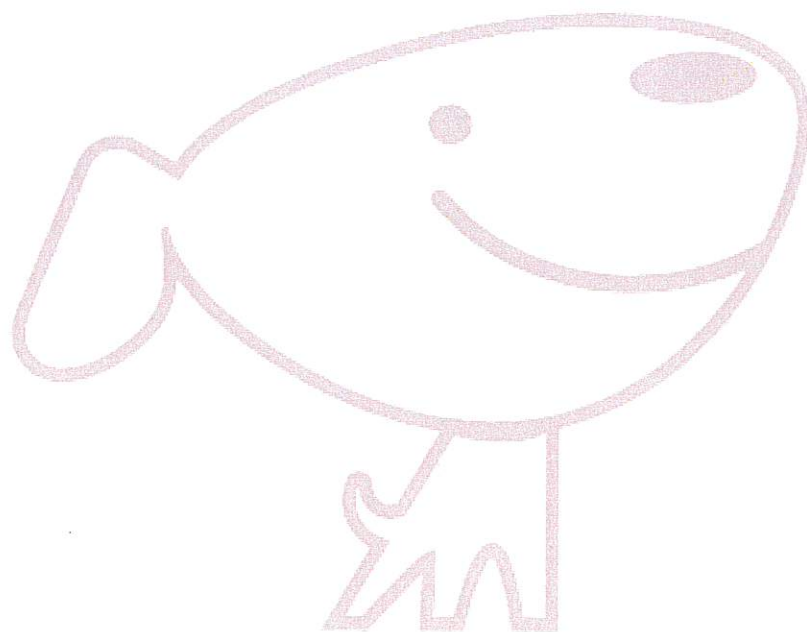
电话：

乙方：京东科技信息技术有限公司

法定代表人或授权代表（签字）：

联系人：

电话：



京东



附件 1:

数据安全保密协议

甲方 1: 宿迁市大数据中心
甲方 2: 宿迁市楚润数据集团有限公司
乙方: 京东科技信息技术有限公司

鉴于:甲乙双方签订了市级政务云统一安全服务项目(以下简称“合同”),在“合同”履行期间(以下简称“合作”期间),甲方向乙方提供的或者乙方在合作过程中所接触到的甲方或甲方业主的网络与业务发展情况、网络拓扑、设备信息、系统账号、用户数据和信息、具有商业价值的信息数据等数据信息。双方同意就上述相关数据信息安全保密达成以下一致:

一、定义

本协议所称“数据信息”系指甲方或甲方业主在合作期间以任何方式(包括但不限于书面、口头、可视方式)向乙方提供的,或在合作过程中乙方所接触到的、以任何形式体现的甲方的任何观点、发现、发明、公式、程序、计划、图表、模型、参数、数据、标准和专有技术秘密,或与合作有关的任何商业、营销、技术、运营、数据或其他性质的资料。

二、保密责任

1. 甲方或甲方业主提供数据信息的行为不构成向乙方授予任何与数据信息相关的专利权、专利申请权、商标权、著作权、商业秘密或其它的知识产权、所有权或其他任何权利。

2. 乙方对数据信息的使用应当满足下列要求:

2.1 乙方应遵守甲方上级单位、甲方及甲方业主内部关于数据安全方面的管理规定等。

2.2 乙方承诺仅在本次合作期间,为合同履行的目的使用数据信息,不为任何其他目的使用数据信息。

2.3 未经甲方的事先书面批准,乙方不得以任何形式或任何方式将数据信息和/或其中的任何部分,披露或透露给任何第三方。

2.4 乙方有义务妥善保管必要的的数据信息,不得私自复制、泄漏或遗失,对于乙方保管的数据信息应采取必要技术保护措施,例如:数据模糊化、金库模式、账号和日志审计等。

2.5 乙方不得依据数据信息,就任何问题,向任何第三方做出任何建议。

2.6 未经甲方同意,乙方不得利用上述数据信息进行新的研究和开发。

3. 乙方有权向其职员透露或使其接触数据信息和/或其中的任何相关部分,这些职员应是参与合作项目运行的项目组人员,前提是乙方向职员透露或使其接触数据信息前已经从该职员获得了至少与本协议保密义务一样严格的保密承诺,并要求在项目结束或职员退出该项目后删除数据信息,不得私人进行备份。

4. 甲方有权在甲方认为必要的情况下收回所提供的数据信息及其使用权,乙方应配合甲方行使上述权利,按照甲方的要求将所控制的数据信息交回甲方、删除或销毁。

三、违约责任和处罚措施

1. 乙方的职员违背保密承诺,未按照本协议的规定使用数据信息,或未遵守甲方数



附件 2:

网络与信息安全责任条款

甲方 1: 宿迁市大数据中心

甲方 2: 宿迁市楚润数据集团有限公司

乙方: 京东科技信息技术有限公司

本条款所包含的安全责任如无特别说明,适用于设备到货、项目验收以及系统运行维护整个过程的各个环节,甲、乙方需要严格执行。

一、安全保障

1. 乙方应提供完善的安全防护措施,包括但不限于防火墙、入侵检测系统、防病毒系统等,保障甲方及甲方业主的数据信息安全,防止数据信息被非法访问、篡改、删除、泄露等。

2. 乙方应定期进行安全检查和评估,及时发现并修复安全漏洞,提高系统的安全性能。

3. 乙方应对其提供的云服务进行持续的安全监控,及时发现并处理任何可能影响甲方及甲方业主数据信息安全的事件。

4. 在项目实施期间,甲方有权通过安全扫描软件或者人工评估等手段,对本次项目新增设备和应用软件进行检查,并给出符合实际的评估结果。一旦发现有重大安全漏洞、后门或者病毒感染,由乙方立即进行免费修补、清除或者采用其他手段消除安全问题。对于违反本规定导致的一切后果,由乙方负全部责任。

5. 在产品投入运行直至退网期间,乙方应及时将通过各种途径所发现的自主研发应用软件或产品在软件代码、功能或配置方面的安全漏洞告知甲方并及时、无偿地提供修补方案并实施修补;或者在甲方发现漏洞后 1 周内最迟不超过 1 个月内,无偿提供修补方案并实施修补。

6. 当加载的安全补丁与乙方所提供的应用系统存在冲突时,乙方原则上应在 1 个月内,最迟不超过 3 个月内,对应用系统进行升级改造。

二、数据保护

1. 乙方应确保甲方及甲方业主的数据信息的完整性、可用性和保密性,不得在未经甲方许可的情况下,复制、修改、删除、泄露甲方及甲方业主的数据信息。

2. 乙方应对甲方及甲方业主的数据信息进行备份,以防数据丢失。备份的频率、方式、存储位置等应符合甲方的要求。

3. 乙方应在数据传输过程中采取加密等措施,保证数据的安全性。

三、应急处理

1. 乙方应建立完善的应急处理机制,对于任何可能影响甲方及甲方业主数据信息安全的事件,应立即启动应急处理程序,及时处理并报告甲方。

2. 乙方应对每一次应急处理事件进行记录和分析,以提高未来的应急处理能力。

四、人员管理

1. 乙方应对参与提供云服务的人员进行严格的安全培训和管理,确保其了解并遵守相关的安全规定。

2. 乙方应对参与提供云服务的人员进行背景审查,以防止内部安全威胁。

五、违约责任

1. 乙方违反本条款的,应当承担违约责任,赔偿甲方因此而遭受的全部损失。

2. 乙方违反本条款的,甲方有权立即终止合同,并要求乙方立即停止使用数据信息,



