2025 年政务云资源租赁和云网安全服务项目政府采购合同

项目名称：2025 年政务云资源租赁和云网安全服务项目

项目编号：JSZC-321300-JXXM-C2025-0007

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》等有关的法律法规，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：2025 年政务云资源租赁和云网安全服务项目。

（二）标的质量：合格。

（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）履行方式：按需交付。

二、合同金额

（一）本合同金额为（大写）：壹仟贰佰伍拾万元（12500000.00 元）人民币或其他币种，不含税金额为（大写）：壹仟壹佰柒拾玖万贰仟肆佰伍拾贰元捌角叁分（11792452.83 元）人民币或其他币种，税款金额为（大写）：柒拾万零柒仟伍佰肆拾柒元壹角柒分（707547.17 元）人民币或其他币种，税率为 6%。

（二）合同清单

序号	服务简述	服务规格描述	单位	数量	单价（元）	总价（元）
1	互联网区-云主机-VCPU	X86 架构，逻辑核心。	核	5500	203.82	1121010
2	互联网区-云主机-内存	X86 架构，云主机内存。	GB	22000	67.94	1494680
3	互联网区-云存储-块存储	X86 架构，支持块存储协议，用于云主机块存储需求。	TB	150	2132.41	319861.5
4	互联网区-云存储-对象存储	X86 架构，支持 S3 等主流对象存储协议，用于非结构化数	TB	400	949.46	379784

		据存储。				
5	互联网区-关系型数据库	PG RDS 服务，支持主备高可用切换，X86 架构，CPU 不低于 2.4GHz（4vCPU），内存不低于 16GB，存储不低于 200GB，IOPS≥5000，最大连接数≥2000 等。	实例	9	6396.51	57568.59
6	互联网区-国产数据库	支持 ARM、国产 X86 等架构，最大连接数≥10000，最大并发数≥1000。	实例	1	8388.55	8388.55
7	互联网区-网络资源	BGP（20Mbps），满足运营商三线网络资源接入，不限 IP 地址数量。	条	29	8040.26	233167.54
8	电子政务外网区-云主机-VCPU	X86 架构，逻辑核心。	核	6000	203.82	1222920
9	电子政务外网区-云主机-内存	X86 架构，云主机内存。	GB	24000	67.94	1630560
10	电子政务外网区-云存储-块存储	X86 架构，支持块存储协议，用于云主机块存储需求。	TB	150	2132.41	319861.5
11	电子政务外网区-云存储-对象存储	X86 架构，支持 S3 等主流对象存储协议，用于非结构化数据存储。	TB	400	949.46	379784
12	电子政务外网区-关系型数据库	PG RDS 服务，支持主备高可用切换，X86 架构，CPU 不低于 2.4GHz（4vCPU），内存不低于 16GB，存储不低于 200GB，IOPS≥5000，最大连接数≥2000 等。	实例	8	6396.5	51172
13	电子政务外网区-主机(信创云)-VCPU	云主机 VCPU,ARM、C86 架构，逻辑核心。	核	1000	451.5	451500
14	电子政务外网区-主机(信创云)-信创内存	ARM、C86 架构，云主机内存。	GB	4000	150.51	602040
15	电子政务外网区-存储(信创云)-信创块存储	ARM、C86 架构，支持块存储协议，用于云主机块存储需求。	TB	100	3966.09	396609
16	电子政务外网区-存储(信创云)-对象存储	ARM、C86 架构，支持 S3 等主流对象存储协议，用于非结构化数据存储。	TB	100	1983.05	198305
17	电子政务外网区-国产数据库	支持 ARM、国产 X86 等架构，最大连接数≥10000，最大并发数≥1000。	实例	1	8388.55	8388.55
18	异地灾备区-存	块存储，SSD 存储介质，用于	TB	100	2132.41	213241

	储	存储灾备数据。				
19	异地灾备区-专线	100Mbps 双路主备。	条	1	52649.83	52649.83
20	异地灾备区-其他	成交人提供数据级异地备份服务，包括但不限于搭建满足使用条件所需的场地（直线距离超 300km）、机柜、计算节点、备份软件、人工、运维服务等。	服务/年	1	136284.34	136284.34
21	同城灾备区-其他	成交人提供数据级同城备份服务，包括但不限于搭建满足使用条件所需的场地（直线距离超 50km）、机柜、计算节点、备份软件、人工、运维服务等。	服务/年	1	118982.68	118982.68
22	其他-桌面云	CPU：4 核，内存：8GB，系统盘：80G，数据盘：1T。	实例/年	1	4629.7	4629.7
23	其他-云文件服务	性能型(SSD 全闪),最大带宽 2GB/s，时延 1ms 左右，单文件系统 IOPS 20000；支持 NFSv3/v4.1。	GB/年	1	11.3	11.3
24	其他-云缓存	支持最大 64 分片；实例规格要求：总容量：1GB，副本：2 个，最大连接数：最大内网带宽：48MB/s。10000，	实例/年	1	535.42	535.42
25	其他-应用负载均衡	支持七层负载均衡服务；实例可用性≥99.95%;内网带宽无限制；最小规格的带宽最大可达 800Mbps，公网带宽取决于负载均衡绑定的弹性 IP 的带宽。	实例/年	1	4323.6	4323.6
26	其他-网络负载均衡	持四层有状态负载均衡服务;实例可用性≥99.95%;内网带宽无限制；最小规格的带宽最大可达 800Mbps，公网带宽取决于负载均衡绑定的弹性 IP 的带宽。	实例/年	1	4323.6	4323.6
27	其他-视频存储	低频存储，用于监控数据存储，数据持久性要求 99.9999999999%，服务可用性要求 99.9%，实时访问 ms 级延迟。	TB/年	1	957.77	957.77
28	其他-GPU 算力	GPU 算力服务需要支持 HPC 高性能计算场景，PF16 性能≥28.26 TFLOPS，PF32 性能≥14.13 TFLOPS，PF64 性能≥7.066TFLOPS。	台	2	18774.95	37549.9

29	其他-数据库 DTS	提供数据传输 DTS 实时数据流服务，支持数据迁移、同步服务，可简单方便的满足数据上云、业务异步解耦、数据异地灾备、业务系统数据流转等业务场景。支持同 VPC 的云数据库或通过专线/内网连接的数据库之间的数据同步，支持库表对象选择，支持“全量+增量”或“增量”两种同步方式。	个	1	12050.68	12050.68
30	其他-消息队列 Kafka	提供 Kafka 的分布式发布订阅消息队列服务，应用于日志收集、流式数据处理、在线和离线分析等场景，提供分布式、高吞吐、可扩展的全托管服务。	套	1	63247.01	63247.01
31	Web 应用防火墙（云 WAF）	支持 WEB 应用攻击防护；支持 CC 攻击自定义规则；支持安全概览；支持 WEB 分析报表；支持自定义恶意 IP 惩罚；支持 OWASP TOP 10 安全检测和防御；业务请求：≥ 5000QPS；业务带宽：≥ 50Mbps；支持一级域名个数：≥2；支持防护域名总数：≥ 20。	实例/年	5	34422.31	172111.55
32	带宽扩展包	Web 应用防火墙业务带宽扩展包，1 个带宽包支持≥50M 业务带宽。	个/年	25	2988.05	74701.25
33	域名扩展包	Web 应用防火墙域名扩展包，1 个域名包支持≥10 个域名（限制仅支持 1 个一级域名）。	个/年	50	2988.05	149402.5
34	Web 应用防火墙（负载均衡服务型）	1）支持 WEB 应用攻击防护； 支持防篡改； 1）支持 BOT 流量管理； 支持 Web 站点合规性 支持 OWASP TOP 10 安全检测和防御； 支持云内子网间 WEB 应用攻击防护，支持无域名防护； 安全报表分析功能。	实例/年	30	5776.89	173306.7
35	主机安全	资产统一管理、资产指纹、主机防勒索、支持容器运行时安全检测、止损脚本管理等功能。	资产/年	860	348.61	299804.6

36	网站威胁扫描	1）支持漏洞检测、UDP 扫描、自定义 web 爬虫深度、扫描报告输出、与安全运营中心联动等功能。	实例/年	1	3585.66	3585.66
37	实例扩展包	网站威胁扫描实例扩展包，扩展实例包，包含一个一级域名，限制对应子域名或者 IP 数量小于 10 个。	个/年	59	597.61	35258.99
38	堡垒机	每个实例支持≥500 资产。支持云上部署方式、用户管理、安全设置、会话审计、操作审计等功能。	实例/年	1	22719.12	22719.12
39	云解析 DNS	支持标准 DNS 解析类型、扩展解析、权重轮询、解析线路等功能。流量防护：≥2G；QPS 防护：≥5WQ/s。	实例/年	9	318.73	2868.57
40	云防火墙	支持：安全策略、NAT 功能、防病毒、应用识别、报文示踪等功能。	实例/年	2	31872.51	63745.02
41	移动安全检测服务	支持 Android 客户端隐私合规检测、IOS 客户端隐私合规检测。	次/年	4	7968.13	31872.52
42	安全事件处置系统	支持发现已知系统漏洞、被攻击资产、当前的告警事件，并及时流转对应业务归属部门及业务归属人，同时监控业务团队进行漏洞修复、资产加固、事件处置的状态，实现告警处置闭环，及时发单到人、追踪跟进解决。支持可视化大屏、安全事件录入、用户管理等功能。	套/年	1	5976.1	5976.1
43	安全运营中心	1）支持容器化部署、安全态势可视化、攻击面概览、安全统一管理、资产管理、安全威胁诱捕、安全威胁检测、产品基线检查、用户行为分析、自动化响应与编排剧本管理等功能。	资产/年	860	348.61	299804.6
44	数据库审计	吞吐量：≥3000 条 SQL/秒；支持数据库数：≥6 个；入库速率：≥200 万/小时；在线存储量：≥200 亿条 SQL 语句。支持数据库兼容性、数据库审计、审计策略与规则、风险扫描、检索等功能。	实例/年	1	12908.37	12908.37
45	安全应用网关	支持业务请求：≥ 5000QPS；WEB 应用攻击防护、敏感信息防泄漏、CC 攻击防护、访问控制与限速、应用网关等功	套/年	1	35856.57	35856.57

		能。				
46	堡垒机	每个实例支持≥500 资产。支持云上部署方式、用户管理、安全设置、会话审计、操作审计等功能。	实例/年	1	22719.12	22719.12
47	数据库审计（电子政务外网）	吞吐量：≥3000 条 SQL/秒；支持数据库数：≥6 个；入库速率：≥200 万/小时；在线存储量：≥200 亿条 SQL 语句。支持数据库兼容性、数据库审计、审计策略与规则、风险扫描、检索等功能。入库速率：≥200 万/小时；在线存储量：≥200 亿条 SQL 语句。支持数据库兼容性、数据库审计、审计策略与规则、风险扫描、检索等功能。	实例/年	1	21513.94	21513.94
48	主机安全	资产统一管理、资产指纹、主机防勒索、支持容器运行时安全检测、止损脚本管理等功能，支持≥2500 个资产。	套/年	1	219123.51	219123.51
49	本地 DNS 解析服务	支持基础 DNS 解析、扩展解析。	套/年	1	8052.79	8052.79
50	安全运营中心	支持≥2500 个主机资产；支持混合多云统一管理、资产管理、安全威胁分析、安全态势可视化等。	套/年	1	1075697.21	1075697.21
51	网站威胁扫描	支持≥2500 个主机资产；支持漏洞检测、UDP 扫描、自定义 web 爬虫深度、扫描报告输出、与安全运营中心联动等功能。	套/年	1	31872.51	31872.51
52	密码服务平台	灵活部署、对称密码（算法：SM4、AES；加密模式：CBC、ECB、GCM）、非对称密码（算法：SM2、RSA2048、密码服务调度、密码服务运行态势可视化、密码设备运行态势可视化、租户与订单管理等功能。	套/年	1	35856.57	35856.57
53	服务器密码机	提供基于国密算法的数据加解密、数据完整性以及密钥生成能力； 算法支持： 支持 SM2、SM3、SM4、SM7、SM9 国密算法；支持 ZUC 流密码算法； 功能要求： 支持对称加解密、非对称加解	套/年	1	31872.51	31872.51

		密、数据完整性计算等基础密码计算功能； 支持密钥安全生成、存储、备份、恢复，采用由国家密码管理局批准的安全芯片； 支持高可用部署，保障业务的连续性； 性能要求： SM2 密钥对产生速率≥38000 对/秒 SM2 签名速率≥ 38000 次/秒 SM2 验签速率≥30000 次/秒 SM2 加密速率≥20000 次/秒 SM2 解密速率≥30000 次/秒 SM3 速率≥850Mbps SM4 加解密速率≥850Mbps。				
54	SSL VPN 安全网关	基于国密算法的 SSL VPN 能力，建立 SSL VPN 通道实现数据安全传输服务，保证数据在通道中的传输机密性与完整性 算法支持： 支持 SM2、SM3、SM4 等国产密码算法； 功能要求： 支持创建多个 SSL VPN 服务，保护 HTTP、TCP 不同的应用服务； 支持主流国际协议，包括但不限于 SSL3.0、TLS1.0、TLS1.1、TLS1.2、TLS1.3； 支持配置根证书校验逻辑，支持权威 CA 签发国际及国密证书，支持自签发证书； 支持标准证书格式包括第三方证书及 CA，支持全中文证书； 性能要求 SM2 新建连接数≥10000 次/秒； SM2 吞吐量≥1Gbps； SM2 并发连接数≥30000； SM2 并发用户数≥30000。	套/年	1	32868.53	32868.53
55	动态令牌认证系统	为应用系统使用人员提供基于国密算法的动态令牌认证功能，在账号认证基础之上增加动态密码，实现双重因子认证，从而有效保护用户认证安全 算法支持：	套/年	1	27888.45	27888.45

		支持 SM2、SM3、SM4 等国密算法； 功能要求： 支持提供认证服务、管理中心、集成动态令牌认证引擎和 RADIUS、Oauth2.0 服务； 支持提供手机令牌形式的客户端使用方式，支持认证用户管理员扫码方式派发激活码； 支持角色管理，管理员可基于用户角色进行授权管理。				
56	文件加密系统	基于国密算法，为操作系统中的文件、目录等提供机密性、完整性保护； 算法支持： 支持 SM2、SM3、SM4 等国密算法； 功能要求： 支持在操作系统内核层实现对文件和数据的加解密； 支持计算和校验文件和数据的消息鉴别码，实现数据完整性检验，检验数据是否被非授权地改变，保证数据的完整性； 支持通过主模块强制访问控制执行和记录模块，拒绝所有未获授权的进程对保护数据的访问； 支持对本项目中对业务系统服务端文件/文件系统的透明加解密服务与完整性校验服务能力； 性能要求： 文件读写性能损耗≤30%。	套/年	1	21912.35	21912.35
57	智能密码钥匙	以硬件设备为数字证书的载体，个人认证密钥在 USBKey 中生成，提高了个人密钥的安全性。实现数字证书的生成存储、数字签名认证、对称加解密、口令认证、内外部认证、数据完整性校验等功能； 算法支持： 支持 SM2、SM3、SM4 等国产算法； 功能要求： 具有加密、解密、签名、验签等功能； 内置 32 位高性能智能安全芯片，内置硬件随机数发生器和	个/年	2	99.6	199.2

		协处理器； 标准 USB2.0 接口设备，兼容支持 USB1.0 接口、USB3.0 接口。				
58	国密浏览器	支持国密算法的 WEB 浏览器； 算法支持： 支持 SM2、SM3、SM4 算法； 功能要求： 支持基于国密算法的数字证书和证书链； 支持标签栏、书签管理、历史记录管理、网页保存、网络代理、无痕浏览、下载等浏览器通用功能。	套/年	2	99.6	199.2
59	个人数字证书	由合法 CA 机构验证个人真实身份后颁发，用于标识使用者在网络应用中的数字身份，防止非法访问、身份仿冒等安全风险； 功能要求： 提供基于国密算法的个人数字证书服务； 数字证书遵循 X.509 Version3 证书格式标准； 数字签名算法支持 SM2，摘要算法支持 SM3，证书请求支持 PKCS#10 格式。	张/年	2	3486.06	6972.12
60	设备证书	由合法 CA 机构颁发，基于国密算法标识设备身份真实性； 功能要求： 提供基于国密算法的设备数字证书服务； 数字证书遵循 X.509 Version3 证书格式标准； 数字签名算法支持 SM2，摘要算法支持 SM3，证书请求支持 PKCS#10 格式。	张/年	2	4980.08	9960.16
61	SSL 站点证书	由合法 CA 机构颁发，用于标识站点身份，建立安全的国密 HTTPS 协议； 功能要求： 提供基于国密算法的 HTTPS/SSL 站点数字证书服务； 数字证书遵循 X.509	张/年	2	8964.14	17928.28

		Version3 证书格式标准； 数字签名算法支持 SM2，摘要算法支持 SM3，证书请求支持 PKCS#10 格式。				
62	硬件动态令牌	1.资质要求：符合 GMT0021《动态口令密码应用技术规范》； 2.内置算法：标准国密 SM3； 3.支持适配其他动态令牌认证系统。	个/年	2	99.6	199.2
63	国密门禁系统	提供 1 套国密门禁管理系统及配套的门禁控制器、读卡器、发卡器和门禁卡等，对物理机房提供基于国密算法的身份鉴别与门禁记录完整性保护服务；门禁管理系统为硬件形态； 包含门禁管理系统 1 套，门禁控制器、读卡器和发卡器各 2 套，门禁卡 20 张； 功能要求： 门禁管理系统具备发卡管理、考勤管理、记录查询、报警提示等功能； 读卡器支持门禁用户身份鉴别，支持 RFID 识别方式； 门禁控制器可控制门数量：2 门，可接入读卡器数量：2 个，支持远程开门功能；支持定时常开门功能； 发卡器读卡距离：≤50mm；读卡时间：≤50ms； 门禁卡支持国密算法，支持门禁用户身份鉴别，读写距离：≤50mm。	套/年	1	11952.19	11952.19
64	国密视频监控系统	包含国密视频监控系统及配套的视频加密系统、国密硬盘录像机、监控硬盘等，对物理机房的视频监控与记录提供完整性保护； 包含视频安全加密系统、国密硬盘录像机、监控硬盘各 1 套；视频加密系统为硬件形态； 功能要求： 视频加密系统内置密码模块，支持国密算法；支持完整性日志以及加密视频的播放；系统支持通用视频系统功能，支持视频历史记录的回看；	套/年	1	14902.98	14902.98

		国密硬盘录像机支持国密算法，支持不低于 1080P 清晰度；系统支持硬盘存满时自动从头覆盖，循环录像； 监控硬盘支持存储 180 天，10T 存储，硬盘接口支持 SATA 接口，经加密处理。				
合计总价含税（元）						12500000

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、合同款项支付及服务期

8.1 服务期：1 年。

8.2 付款方式：合同签订且甲方 2 在收到乙方发票后 10 个工作日内，支付合同总金额的 20%作为预付款；服务期满且经甲方考核、第三方机构评估及最终验收合格，根据相关结果和要求支付余款（无息）。

8.3 根据全年各项服务实际使用量计算。

资金支付的主体：宿迁市楚润数据集团有限公司。

资金支付的条件：满足相应阶段的要求且甲方 2 收到甲方 1 对应款项和乙方发票。

8.4 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 乙方所提供云服务须符合《宿迁市政务云管理暂行办法》。

10.2 乙方所提供云服务须支持资源动态实时监测、弹性调整、多云管理。

10.3 乙方成交后，应协助甲方与前云服务商做好衔接工作，包括但不限于人员、网络、资源使用、业务系统迁移、数据迁移和安全服务等方面的工作。系统迁移必须保证业务系统连续稳定安全运行的前提下完成迁移工作，由乙方协助甲方与前乙方协调解决。

10.4 云服务包含但不限于虚拟机、NAT 网关、负载均衡、域名解析、基础安全防护包等以及满足需要的机柜、带宽等必备配套并满足信息系统安装部署需求（信创改造除外），基础安全防护包应提供主机监控、堡垒机（含运维 VPN 接入）、应

用控制、防病毒网关、IPS、主机病毒防护等；云主机应支持 VCPU 与内存按包括但不限于 1:1、1:2、1:4、1:8 等比例按用户需要灵活配置。本项目中涉及的堡垒机、跳板机使用的云资源不纳入云资源统计和计费范围。

10.5 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、VPN 网关、密码服务平台等。

10.6 本项目需求清单中“（一）互联网区域算力资源”和“（二）电子政务外网区域算力资源”服务范围为宿迁市级政务云相关服务，包括但不限于：云平台运维费用、云平台与宿迁市电子政务外网对接的费用、培训、数据安全驻场服务、安全运营等服务费等，不涉及云平台外部非采购人所属网络或专用网络接入云平台的相关专线费用、专线端口占用费用、托管设备上下架费用等。

10.7 本项目需求清单中“（四）互联网区安全资源”和“（五）电子政务外网区安全资源”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、项目实施要求

11.1 乙方在成交后应按照甲方要求，提供数据相关服务。要求乙方对本项目实施计划及实施方案、工期进度安排、云服务的重点、难点问题，包含上云系统情况、数据情况、业务使用情况等内容，能够提出可行方案。

11.2 乙方在成交后应协助甲方对本服务全过程进行管理，合理安排项目组织管理工作。

11.3 提供驻场服务，包括 1 个项目管理岗位，主要负责统筹宿迁市政务云运营管理工作；架构师 2 个岗位，主要负责业务系统上云全生命周期管理相关工作；数据分析师 1 个岗位，主要负责台账管理及数据报告输出相关工作；运维工程师 2 个岗位，主要负责政务云平台运维相关工作；安全运维工程师 5 个岗位，主要负责政

务云安全相关工作。

11.4 乙方应配合甲方总结、展示宿迁市政务云工作中的新思路、新举措、新经验和新成果，积极参与国家级、省级的各类评优评选，营造良好的创新创优氛围。

11.5 乙方在服务期内应协助甲方进行信息化系统信创改造、信创服务器托管部署等工作。

十二、云平台架构设计要求

要求乙方云平台采用高可用部署架构，包括管控面高可用、网络转发面高冗余、服务器磁盘冗余配置，存储服务实现数据多副本保存等。

12.1 在网络架构支撑上，Spine 交换机和 Leaf 交换机等都采用堆叠架构，服务器双上联到 Leaf 交换机，保障整个网络架构的高可靠；

12.2 云平台底层所有服务器系统盘均做 RAID1，云硬盘资源节点由于从软件层面保证三副本；

12.3 云存储服务采用分布式架构，数据采用三副本进行存储。

十三、安全运营要求

13.1 安全运营服务：根据甲方要求，提供日常现场驻守服务，服从甲方管理。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，供市大数据中心管理参考。

13.2 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。

13.3 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。

13.4 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。

13.5 配置实施服务：本项目涉及的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。

13.6 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。

13.7 安全内控服务：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。

13.8 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。

13.9 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。

13.10 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。

13.11 安全事件处置服务：提供安全事件处置服务，在政务云遭遇网络攻击、木马病毒、数据窃取等黑客入侵事件时，能够提供包括抑制止损、事件分析、系统加固、事件溯源等应急响应服务，降低安全事件对政务云造成的影响与损失。

十四、数据灾备要求

14.1 异地灾备要求：

（1）乙方应设计科学合理并且可行的异地灾备方案，包括选址、灾备环境、安全等。

（2）异地灾备要求距离现有主数据中心间距离保证在 300KM 以上，同时还应做

到不在一个地震带，不在同一电网，不在同一江河流域。

（3）异地灾备应有运行维护管理能力，包括介质存取、验证和转储管理制度，以及对备份数据进行定期的有效性验证。

14.2 同城（宿迁市）灾备要求：

（1）乙方应设计科学合理并且可行的同城灾备方案，包括选址、灾备环境、安全等。

（2）同城灾备要求距离现有主数据中心间距离保证在 50KM 以上

注：同城灾备区的存储与专线由采购人协调泗阳县政务云提供。中标人需协助做好同城地灾备区相关工作。

十五、机房环境要求

制定机房环境及配套的服务方案，包含机房空间、空调、UPS 电源、监控、消防、安防、双路供电等情况。

15.1 乙方所使用机房应符合国家相关标准的要求；

15.2 机房应设专用可靠的供电线路，计算机系统的电源设备应提供稳定可靠的电源。供电电源设备的容量应具有一定的余量。

十六、运维服务要求

16.1 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。

16.2 需提供 7*24 小时服务，乙方应根据甲方业务需要配备在甲方指定地点驻场服务团队，并配备足够数量的驻场服务人员。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。

16.3 在信息系统出现重大异常或其他紧急情况，对政务云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，将相关情况告知到使用单位。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。

16.4 乙方应明确服务团队各工作岗位的设定和责任边界，上岗前应取得甲方同意，不得随意减配人员数量，不得降低人员质量要求。

16.5 在成交后配合甲方根据需要进行宿迁市政务云网应急预案日常演练和实战流程。同时，每季度开展不低于一次的全市政务云和电子政务外网网络安全漏洞扫描和渗透测试服务。

16.6 按照宿迁市政务云的相关项目管理规范积极开展岗前培训，围绕《宿迁市政务云管理暂行办法》结合线下线上工作流程，配合甲方明确政务云申请、审核、开通、部署、测试、上线、变更和退出闭环工作流程，协助甲方对云资源升配、降配、回收等技术保障工作。

16.7 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，乙方须保证所提供的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。

十七、安全审查和保密要求

上云系统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。

17.1 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损失，并根据国家有关保密规定追究责任。

17.2 密码应用安全性要求

按照《中华人民共和国密码法》及国家商用密码管理规定，配合开展密码应用安全性评估工作，本项目要满足国家、省、市密码管理有关法律法规和标准规范要求。

十八、考核评价要求

18.1 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。

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

18.3 根据《宿迁市政务云运营考核细则》，按季度开展政务云服务商服务质量考核与云资源使用情况审核，提升精细化管理水平。合同期满，甲方根据全年考核情况进行扣款。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≥90 分，不扣费用；

2） 90 分＞考核评价得分≥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%；

考核细则如下：

打分细则（符合甲方规范要求，包括但不限于）	分值
1、乙方的机房建设和配套设施符合中国质量认证中心（CQC）颁发的 A 级数据中心认定标准	每出现一次不符合扣 5 分
2、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 5 分
3、乙方应服从甲方的管理制度	每出现一次不配合扣 5 分
4、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 1-5 分
5、乙方应按周、月、季、年出具运维报告，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
6、人员出现离岗、超时（10 个工作日）未安排同等条件或以上人员到岗补充等情况	扣 10 分/人.次，每超过 10 个工作日未完成人员到岗的扣 5 分一次
7、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
8、乙方不得未经用户单位授权对用户账号下云服务器进行管理操作，变更账号管理权限，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 1-10 分
9、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 1-5 分
10、乙方应提供良好的服务态度，不得恶意骚	每发生一次按情况严重程

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	度扣 1-5 分
11、乙方需对发生的故障进行抢修，保持甲方业务的可用性，应在 30 分钟内响应并告知甲方。	每发生一次超时按情况严重程度扣 1-10 分
12、乙方应根据甲方最新印发的《宿迁市政务云管理暂行办法》中故障处理时限处理故障，并形成事故分析报告。	每发生一次超时按情况严重程度扣 1-10 分
13、配合甲方做好申请单位的需求受理、评估上云部署方案和资源需求用量，参与评审并给出专业意见。	每出现一次需求评审不配合或评估不准确，根据情况影响程度扣 1-5 分
14、甲方提出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 1-5 分
15、根据甲方要求，结合政务云的运行系统和资源用量，定制开发云资源监测平台，并协助甲方进行资源监测（包括物理资源和云化资源），定期出具监测报告，确保甲方和使用单位能够监测相关上云系统运行情况，及时掌握云资源消耗占比，并给出资源优化建议。	甲方提出需求，乙方根据提出的时间节点予以提供配合，出现一次不配合或监测平台无法正常使用（不可抗力除外），根据情况影响程度扣 1-10 分。甲方使用监测系统过程中，发现数据不准确的，每次扣 1 分。
16、根据甲方要求，做好资源回收工作，并协助	每出现一次资源回收不配

甲方沟通使用单位，及时、平稳、高效回收资源。	合或不及时，根据情况影响程度扣 1-10 分
17、配合甲方做好政务云资源申请相关材料的归档。	每出现一次不配合或不及时，根据情况影响程度扣 1-5 分
18、乙方需对政务云平台配合开展等保测评。	等保测评分数低于 70 的扣 5 分。
19、政务云开展等保测评扣分部分未在时限内整改或整改不达标的	扣 5 分一次。
20、对攻防演练中出现的问题未及时处理的	扣 5 分一次。
21、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 1-5 分
22、因乙方造成的政务云故障。酌情扣分。	一级故障扣除 20-40 分，二级故障扣除 10-20 分，三级故障可根据实际情况酌情扣除 1-10 分。
23、对通报情况进行扣分	若因乙方原因造成甲方被通报批评，每发生一次扣 5 分。
24、因团队管理出现劳动纠纷、不稳定等引发服务质量下降、中断等情况或造成舆论导致甲方形象受损的	按照影响程度扣 10-20 分。
25、对甲方及使用单位的资源维护、培训、服务	每出现一次按情况严重程

不到位，导致客户投诉，造成一定社会影响	度扣 2-5 分
26、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	
27、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）	
28、未将客户处发生网络安全的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	
29、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	
30、对客户的询问不予说明清楚、含糊其词，引起用户单位误解的	
31、协助甲方获取江苏省数据要素 X 大赛或国家级数据要素 X 大赛奖项	每个省级奖项加 5 分，国家级加 10 分
32、乙方协助甲方获得市级或以上领导批示表扬，市级或文件表扬的	每次加 5 分

十九、项目验收

19.1 根据全年各项服务实际使用量计算。

19.2 甲方对乙方考核评价结果（考核评价见第十八项）作为验收参考依据。

19.3 项目服务期结束后，甲方根据服务情况，组织最终验收并出具加盖甲方公章的验收报告。

19.4 甲方在服务期内每个自然季度结束前 5 个工作日对当季度服务资源盘点报告进行确认并加盖甲方公章。

19.5 甲方依法组织履约验收工作。

19.6 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。

19.7 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。

19.8 如有必要，甲方邀请参加本项目的其他乙方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。

19.9 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。

19.10 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。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。

二十、违约责任

20.1 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。

20.2 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。

20.3 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，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。

20.4 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。

20.5 甲方逾期退还履约保证金的违约责任：除应当退还履约保证金外，还应当按中国人民银行同期贷款基准利率上浮 20%后的利率支付逾期资金占用费，但因乙方自身原因导致无法及时退还的除外。

二十一、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，采购人依据实际情况对乙方进行补偿救济。

二十二、不可抗力事件处理

22.1 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。

22.2 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。

22.3 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。

二十三、解决争议的方法

23.1 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。

二十四、合同生效及其它

24.1 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。

24.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

24.3 本合同正本一式陆份，具有同等法律效力。

24.4 招标文件、投标文件是本合同的组成部分，均需履行。

24.5 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：

法定代表人或授权代表（签字）：李波

联系人：薛增原

电话：18036993621

甲方 2：

法定代表人或授权代表（签字）：胡鹏

联系人：李明

电话：18860805635

乙方：

法定代表人或授权代表（签字）：

联系人：王广城

电话：18451468074

签订日期：2025 年 10 月 17 日

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 2025 年政务云资源租赁和云网安全服务项目合同（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，或未遵守甲方数据安全管理规定造成数据信息泄露，或向第三方披露数据信息，或依据该等数据信息向第三方做出任何建议，或利用数据信息进行新的研究开发，都被视为乙方违反本协议。

2. 如任何乙方违反本协议，甲方有权要求乙方承担下述各项违约责任，同时甲方有权以书面形式单方面通知乙方终止合作：

2.1 立即停止违反本协议的行为；

2.2 采取一切有效措施防止数据信息泄露范围继续扩大；

2.3 向甲方支付违约金伍拾万元，违约金不足以赔偿甲方损失的，乙方应承担因此给甲方造成的直接损失，包括但不限于甲方因此受到的直接、间接、连带、特殊损失，甲方为调查乙方违约所支出的费用，甲方因乙方违反本协议而导致的任何支出、罚金和费用等。

2.4 甲方有权利采取将乙方加入甲方合作负面行为名单，报送相关行业管理部门将乙方加入行业负面行为名单等措施。

四、数据使用期限

除法律明确规定外，本协议规定的数据信息的使用期限仅限于“合作”过程中（合同有效期内）使用，合作结束后除非甲方书面授权，乙方应将所控制的数据信息交回甲方、删除或销毁。数据信息的保密责任期限为自本协议生效之日起至数据信息失去其保密性质并为公众所知悉之时为止，不因“合作”终止或解除（合同过期）而结束。

五、免责条款

由于地震、水灾、火灾或政策法规变化等不能预见、不能避免、不能抗拒的原因，导致甲乙双方或一方不能履行或不能完全履行本协议项下的有关义务时，甲乙双方相互不承担违约责任；在不可抗力影响消除后的合理时间内，一方或双方应当继续履行本协议。

六、本协议作为合同附件，生效起止时间同合同。本协议需经双方法人代表（或法人代表委托人）签名并盖章，与所签合同具有同等法律效力。合同正本一式陆份，甲方 1 贰份，甲方 2 贰份，乙方贰份，均具有同等法律效力。

甲方 1 名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日

甲方 2 名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日

乙方名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日

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安全评估，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网安全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网安全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网安全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，乙方应当立即将其所持有的所有数据信息以及所有副本返还给甲方，并删除其系统中的所有数据信息。

本协议作为合同附件，生效起止时间同合同。本协议需经双方法人代表（或法人代表委托人）签名并盖章，与所签合同具有同等法律效力。合同正本一式陆份，甲方 1 贰份，甲方 2 贰份，乙方贰份，均具有同等法律效力。

甲方 1 名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日

甲方 2 名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日

乙方名称：_____（盖章）

法定代表人或授权代表：_____

签约日期：2025 年 10 月 17 日