朝阳区电子政务云平台密码资源池建设项目合同

项目名称：朝阳区电子政务云平台密码资源池建设项目

签订地点：北京市朝阳区

签订时间：2018 年 10 月 17 日

甲方（购买方）：北京市朝阳区数据局

乙方（供货方）：京闽数科（北京）有限公司

根据《中华人民共和国民法典》规定，甲乙双方本着公平自愿、平等互利、诚实信用的原则，经友好协商，就朝阳区电子政务云密码资源池建设项目物资采购事宜达成如下协议：

第一条：标的物

物资具体名称、规格型号、生产厂商、品牌商标、材质、单价、数量详见合同附件。

第二条：合同价款

合同总价款为 2,462,606.60 元，大写：贰佰肆拾陆万贰仟陆佰零陆元陆角。

本合同适用税率为硬件及成品软件产品为 13%，服务为 6%。

第三条：结算及付款方式

3.1 首付款：合同生效后 30 个工作日内，甲方向乙方支付合同数额的 50.59% ，为（人民币）：1,245,900.00 元，大写：人民币壹佰贰拾肆万伍仟玖佰元整。

3.2 尾款：本项目验收合格后，甲方向乙方支付尾款（合同数额的 49.41%），为（人民币）：1,216,706.60 元，大写：人民币壹佰贰拾壹万陆仟柒佰零陆元陆角。甲方付款前，乙方提供等额正式发票。

3.3 履约保证金:在合同签订后【30】个工作日内由乙方向甲方提交合同总价款【10%】的履约保证金或者保函，共计人民币【246,260.66】元(大写:【人民币贰拾肆万陆仟贰佰陆拾元陆角陆分】)。本合同履约保证金或保函于项目终验验收合格后将自动转为质量保证金或保函。在 5 年质保期内无质量事故的，质保期满后返还质量保证金或保函。

本项目质量保证期限：提供硬件产品 五 年免费质保，软件产品提供 三 年免费质保，包括产品质量、使用等问题，时间从项目验收通过之日开始计算。

第四条：履行期限、地点和交付方式

4.1 交货时间： 合同签订 3 个月内所有货物交货完成。

4.2 交货地点： 甲方指定地点。

4.3 调试周期： 设备到货阶段完成后 6 个月内完成设备调试。

4.4 试运行周期： 设备调试完成后进行为期 3 个月试运行。

4.5 运输费承担：设备运输费由乙方承担。

第五条：产品包装及质量要求

5.1 包装方式：出厂标准包装（内含安装配件、合格证、装箱单、使用说明书及产

品质量保证书）。甲方对包装有特殊要求时，乙方应在保证货物质量的前提下满足。

5.2 双方关于包装物回收的约定：按照甲方要求处理

5.3 质量要求：达到生产标准并具备产品使用说明书的使用功能。

第六条：验收

系统上线后，乙方向甲方提出验收申请后，甲方组织验收工作开展。

第七条：售后服务及安装

售后服务要求，乙方应针对本项目提供详细的维护与售后服务方案，建立完善的售后服务体系。项目建设完验收成后，提供完整的系统操作使用手册、运行维护手册、软硬件安装测试记录等相关文档，为系统使用人员操作、维护提供帮助。使其具备发现、排除一般问题或故障的能力。系统经过最终验收进入质保期，建设厂商提供相应硬件五年，软件三年质保服务，质保期服务包括但不限于：保证现有的信息系统的正常运行，对于质保期内发现的系统问题及时进行排查、解决、优化，乙方应提供技术支撑及售后服务团队，同时提供灵活、多样的通信手段，7*24 小时的响应服务，保证在任何时候都能及时响应用户要求。在质保期内，提供软件版本更新及升级服务。提供完备的事件响应流程，可提供多种快捷方式，及时准确地解决系统开通运行后出现的各种问题。在系统完成质保期后，根据系统运行情况，进行软件系统运维服务期，服务期内保证现有的信息系统的正常运行，降低整体管理成本，提高网络信息系统的整体服务水平。同时根据日常维护的数据和记录，提供信息系统的整体建设规划和建议，更好的为用户的信息化发展提供有力的保障。

第八条：甲乙双方权利义务

8.1 甲方在符合付款条件时，及时履行付款义务。

8.2 乙方保证所有项目符合国家标准以及行业标准。

8.3 乙方严格遵守中华人民共和国法律、法规及合同对有关技术资料及技术的要求。

8.4 乙方确保其提供的本合同项下的所有服务所涉及的产品、技术、资料不会侵犯第三方的知识产权或所有权，否则由此造成的损失，由乙方承担全部责任。

8.5 乙方安排的与甲方对接工作的人员在服务期间，因故意或过失给甲方造成相应损失的，乙方应承担相应的赔偿责任。

第九条：合同的变更和解除

9.1 如合同履行过程中出现变更，可以另行签订补充协议，该协议与本合同具备同等法律效力。

9.2 若发生如下情形，可以解除本合同：

9.2.1 发生地震、火灾、战争、动乱、暴风雨雪等恶劣天气不可抗力时，致使无法实现合同目的；或

9.2.2 甲乙双方协商一致，可以解除合同；或

9.2.3 本合同约定合同解除的情形。

第十条：违约责任

10.1 乙方违反本合同约定义务的，甲方有权要求乙方在指定期限内采取弥补措施，乙方未能弥补的，视为乙方违约，乙方应向甲方支付相当于合同总金额【百分之三】的违约金。

10.2 乙方延期履行的，每延期一日，按合同总金额【千分之三】向甲方支付延期履行违约金。

10.3 因乙方过错造成甲方或第三方损失的，乙方应赔偿甲方或第三方全部损失。

10.4 甲方有权直接在未支付的合同总金额中扣除本条约定的违约金及赔偿金，不足部分由乙方补齐。

第十一条：争议处理

本合同履行过程中如发生任何争议，由甲乙双方协商解决。双方友好协商解决不成的，任何一方可向北京市朝阳区人民法院起诉。

第十二条：其它条款

12.1 本合同自甲乙双方代表签字并加盖公章后生效。

12.2 本合同壹式肆份，甲乙双方各执贰份，具备同等法律效力。

12.3 如甲方因为机构调整变更主体，由变更后的主体继续履行本合同项下的内容。

附件 1：《货物/服务清单》

附件 2：验收标准

附件 3：合作伙伴廉政协议

附件 4：乙方账户信息

甲方：（盖章）北京市朝阳区数据局

授权代表人（签字）

日期：2025.10.27

乙方：（盖章）京闽数科（北京）有限公司

法定代表人或者授权代表人（签字）

日期：2025.10.27

附件 1：《货物/服务清单》

序号	货物/服务名称	品牌	规格、型号	单价（元）	数量	合价（元）	税率	质保期
1	云服务器密码机	三未信安	2U、SJJ1601 V4P2	371704.20	4	1486816.80	13%	五年
2	IPSec/SSL VPN 综合安全网关	三未信安	1U 、 SecGW G1300 V2	95245.50	2	190491.00	13%	五年
3	时间戳服务器	三未信安	2U 、 SFJ1803-G V4	91198.80	1	91198.80	13%	五年
4	密码服务平台	三未信安	CCSP V1.0	200000.00	1	200000.00	13%	三年

序号	货物/服务名称	品牌	规格、型号	单价（元）	数量	合价（元）	税率	质保期
5	数据库加密模块	三未信安	CCSP V1.0	98700.00	1	98700.00	13%	三年
6	密钥管理模块	三未信安	CCSP V1.0	98700.00	1	98700.00	13%	三年
7	签名验签模块	三未信安	CCSP V1.0	98700.00	1	98700.00	13%	三年
8	云上系统接入服务	京闽数科	/	6600.00	30	198000.00	6%	/
合计						2462606.60		/

一、云服务器密码机规格参数要求

序号	指标项	性能/功能
1	硬件要求	2U 机架式设备，采用国产硬件平台；冗余电源，支持交直流电源输入；前面板支持液晶屏显示网络状态等信息；至少提供 2 个千兆电口，2 个万兆光口。
2		设备具备第三方具有资质机构出具的高温存储、低温存储、高温运行、低温运行、振动试验及跌落试验环境可靠性检测报告。
3		支持 IPV4 和 IPV6 网络双栈配置
4	算法与接口	支持 SM1、SM2、SM3、SM4、SM9 国密算法；支持 RSA、AES、3DES、ECDSA，DSA、SHA1、SHA256、SHA384、SHA512 算法；对称算法支持 ECB，CBC、CTR 和 GCM 算法模式；
5		支持 GMT 0018、GMT 0019、PKCS#11、MS-CSP、JCE 标准接口，SJF 接口和雷卡指令集接口；
6	云服务器密码机管理要求	支持 GMT 0088 云服务器密码机管理接口、ManageOne 运维 Restful API 接口；
7		云密码机虚机支持通过 VXLAN、地址映射等方式与租户 VPC 打通；
8		设备密钥管理和密码运算功能均由设备内的密码卡完成，设备所采用 PCI-E 密码卡和智能密码钥匙具备二级模块《商用密码产品认证证书》，同时密码卡、整机

序号	指标项	性能/功能
		及配件智能密码钥匙为同一品牌。
9		支持用户间资源逻辑隔离，支持资源弹性扩展；
10		支持在线升级功能，并支持对在线升级包进行数字签名验证，保证升级包的真实性、完整性。
11	云服务器密码机性能要求	单台设备可虚拟≥32 台虚拟设备； SM1(包长：32KB)加解密速率≥8000Mbps、 SM4(包长：32KB)加解密速率≥8000Mbps、 SM3(包长：32KB)≥8000Mbps、 SM2（256 位）密钥对生成速率≥14000 TPS、 SM2（256 位）签名速率≥230000TPS、 SM2（256 位）验证速率≥120000TPS、 SM2（256 位，包长 32B）加密速率≥50000TPS、 SM2（256 位，包长 32B）解密速率≥60000TPS。 SM2（256 位，包长 30KB）加密速率≥1700Mbps、 SM2（256 位，包长 30KB）解密速率≥1700Mbps。

序号	指标项	性能/功能
12	产品资质	★投标产品具备商用密码产品认证证书。
13		投标产品具备网络安全专用产品安全检测证书。
14		为确保与国产环境的兼容性，至少具备海光、飞腾、鲲鹏等两个或两个以上国产CPU的适配能力认可证书；至少具备银河麒麟、统信、OpenCloudOS等两个或两个以上国产操作系统的适配能力认可证书；至少具备达梦、人大金仓等两个或两个以上国产数据库的适配能力认可证书；至少东方通、金蝶、金格等两个或两个以上国产中间件的适配能力认可证书。

二、IPSec/SSL VPN综合安全网关规格参数要求

序号	指标细项	指标要求
1	产品资质	★投标产品具备国家密码管理局颁发的有效期内的商用密码产品认证证书，同时遵循国密标准GM/T 0025《SSL VPN网关产品规范》、GM/T 0023《IPSec VPN网关产品规范》、GM/T 0028《密码模块安全技术要求》第二级要求
2		投标产品具备网络安全专用产品安全检测证书。
3	规格要求	标准1U机架式设备，采用国产硬件平台。CPU≧8核，内存≧16G，硬盘为SSD ≧ 120G。

序号	指标细项	指标要求
		1+1 冗余电源。RJ-45 10/100/1000Mb≧6 个,千兆光口≧4 个，支持万兆光口扩展。
4	设备性能	IPSec VPN 最大并发隧道数≥10000，每条隧道都有业务且不丢包； IPSec VPN 最大吞吐率≥15Gbps，包长 64 字节到 1428 字节； SSL VPN 每秒新建连接数≥32000； SSL VPN 每秒并发连接数≥220000； SSL VPN 最大吞吐率≥2.5Gbps，包长 64 字节到 1428 字节
5	算法支持	★支持国密与国际 SSL 算法套件及协议，支持 SSL3.0、TLSv1.0/v1.1/v1.2/v1.3、GMTLSv1.1，支持国密算法套件 ECC_SM4_SM3、ECDHE_SM4_SM3、ECC_SM4_GCM_SM3、ECDHE_SM4_GCM_SM3（对应 ECDHE、ECC 的算法为 SM2）等算法套件
6	客户端支持	具备客户端软件，客户端支持 UKEY 认证方式且适配国产和非国产操作系统客户端 Windows、Linux、统信、银河麒麟系统等；在 UKEY 认证基础上支持匿名模式和用户名口令再次认证模式
7	SSL 功能要求	支持 LDAP、HTTP、手工上传等多种方式更新 CRL 黑名单，支持国密双证书体系，支持动态认证功能、多站点证书功能和第三方签发证书。
8		支持管理员的三权分立功能包括系统管理员、系统操作员和系统审计员，支持基于

序号	指标细项	指标要求
		数字证书认证的智能密码钥匙方式进行系统管理和日志记录完整性保护，满足密评的合规。
9		支持 B/S 和 C/S 架构应用，支持 FTP、Telnet、远程桌面以及通用的 C/S 应用
10		支持应用重定向功能即在有防火墙 NAT 映射的情况下正常访问有重定向的网站，支持网络桥接功能实现大规模复杂网络环境下跨网段实现广播包传输。
11		支持多种优秀的负载算法，可以对后端多个应用服务进行负载，包括轮询、简单轮询、IP 哈希、最少连接和最小响应等。
12		支持 SSL 通道加速功能，包括 WEB 缓存、连接复用、异步 I/O、Cache、Pool 机制、HTTP 压缩等。
13		支持对 CPU、内存、磁盘容量、SSL 代理数、IPSec 隧道数、网络吞吐量等资源情况进行监控和展示，便于系统的维护和问题定位。
14	IPSec 功能要求	支持 IPSec IKE 国密算法和国密协议；支持 IPSec NAT 穿越；支持基于 IP 的所有网络应用
15	高可用能力	支持集群部署，主备机器间自动同步数据，在出现单点故障时主备自动切换，防止单点故障。产品还应支持被第三方负载均衡器进行负载。

序号	指标细项	指标要求
16	管理能力	支持基于数字证书认证的 UKey 方式进行系统管理；也能支持用户名口令认证方式。
17		支持本地根证书管理，支持用本地根证书给 P10 签发证书，支持给 UKey 签发证书。
18		支持证书导入，支持生成 P10 证书请求，支持第三方 CA 签发的证书及全中文证书；支持导入多种格式的证书，支持导入 PEM、DER、PKCS12、BASE64 格式证书；支持导入 GM/T 0009、GM/T 0016 国密规范格式的加密证书密钥。
19		支持备份恢复，备份网关所有数据，备份数据使用备份密钥加密，备份密钥保护支持门限秘密共享技术分割备份密钥并将分量存储在 UKey 中，以及口令保护两种模式，使用 UKey 进行恢复时使用一半以上 UKey 即可进行恢复。
20	监控告警	支持展示设备启动信息、CPU、内存、磁盘、SSL 代理数、IPSec 隧道信息、网口信息、策略信息、网络信息、证书信息等；支持展示整机的总吞吐和指定网卡的吞吐信息；
21		支持以邮件及日志方式对系统问题进行告警，能够配置 CPU、内存、硬盘、网口状态、隧道状态、连接数、系统关键服务等告警规则，可根据阈值、异常持续时间、正常持续时间配置告警规则；达到告警规则条件时可触发相关告警。

三、时间戳服务器规格参数要求

序号	指标细项	指标要求
1	产品资质	★投标产品具备《商用密码产品认证证书》
2		投标产品具备网络安全专用产品安全检测证书。
3	设备形态	2U 机架式设备
4	硬件要求	冗余电源，支持交直流电源输入
5		冗余硬盘，支持数据冗余备份
6		前面板支持液晶屏显示设备信息
7		至少提供 2 个网络端口
8		支持万兆网口扩展
9	算法支持	支持 256 位 SM2 公钥密码算法。
10		支持 1024、2048 位的 RSA 公钥密码算法。
11		支持 SM3 摘要算法。
12	时间戳管理功能要求	同时支持签发和验证 RSA、SM2 算法的时间戳。
13		支持通过 NTP 协议从时间源同步系统时间，时间精确到毫秒。
14		支持时间戳服务器证书管理，包括新增、更新、下载、查询等。

序号	指标细项	指标要求
15		支持时间戳和历史时间戳存储、查看、下载等管理。
16	安全功能要求	支持采用基于数字证书的硬件密码钥匙（USBKEY）“双因子”认证方式实现管理人员的身份鉴别。
17		支持基于 https 实现远程管理和配置。
18		支持白名单管理。
19		支持对数据库的备份管理，系统管理员可方便的在管理控制台完成系统备份操作，可下载到本地进行妥善保存。
20	管理功能要求	支持系统用户管理：支持根据管理、审计分立原则划分用户角色及权限，包括管理员、审计员。
21		支持所有的关键操作均记录日志，可对系统中所有的日志进行查询和审计。
22		支持配置系统网络等。
23	性能要求	支持存储百万级时间戳。
24		SDK 申请 RSA 时间戳性能≥4000TPS SDK 验证 RSA 时间戳性能≥6500TPS SDK 申请 SM2 时间戳性能≥6000TPS

序号	指标细项	指标要求
		SDK 验证 SM2 时间戳性能≥11000TPS 申请并发数≥50，验证并发数≥50 申请最大连接数≥300，验证最大连接数≥300

四、签名验签模块规格参数要求

序号	指标细项	指标要求
1	签名验签模块	提供密码服务平台的签名验签服务，支持 SM2、RSA 签名验签算法，支持多信任域、多应用、数字签名和验签、数字信封加密和解密、签名的数字信封加密和解密，含 1 套授权。

五、密钥管理模块规格参数要求

序号	指标细项	指标要求
1	密钥管理模块	提供密码服务平台的密钥管理服务，支持国密算法的密钥全生命周期管理、多级密钥生成与管理、证书导入与管理、数据库加密密钥的统一管理，含 1 套授权。

六、数据库加密模块规格参数要求

序号	指标细项	指标要求
1	数据库加密模块	提供密码服务平台的数据库加密服务，支持 SM3，SM4 国密算法，支持关系型数据库的密钥管理、关系型数据库的机密性和完整性保护、关系型数据库字段加密、列加密、表加密、库加密，并无需数据库改造，支持 Postgres、MySQL、Mariadb、达梦、人大金仓、OpenGauss、PostgresSql、瀚高、Percona、TiDB、OCeanbase、Vastbase、Gbase、MogDB、神舟通用、Gaussdb、TDsql 等数据库透明加密，含 1 套授权。

七、密码服务平台规格参数要求

序号	指标细项	指标要求
1	加解密服务	支持 SM1、SM2、SM4、SM9、DES/3DES、AES、RSA、ECDSA 算法等国内和国际密码算法；
2		支持提供基于双 WNG8 物理随机源的随机数
3		支持 RESTFUL 接口协议；
4		支持采用账户/口令或者数字证书的方式进行接口级别的应用系统身份鉴别，确保密码设备不会被非法调用；
5	签名验签服务	支持 SM2、RSA 签名验签算法；
6		支持 RESTFUL 接口协议；

序号	指标细项	指标要求
7		支持采用账户/口令或者数字证书的方式进行接口级别的应用系统身份鉴别，确保密码设备不会被非法调用；
8	数据库加密服务	支持国际数据库，如 Oracle、MySQL、SQL Server 等，支撑国产数据库，如达梦、人大金仓、OpenGuass 等数据库
9		支持数据库字段级数据加密，确保数据机密性；
		支持应用免改造的国密算法透明加密；
10		支持对历史数据的自动转加密，适用于已有数据的生产环境；
11		支持对数据库定义第三方权限访问策略；
12	密钥管理服务	支持密钥管理支持 KMIP（Key Management Interoperability Protocol）标准规范，对称密钥和非对称密钥的激活、撤销、更新、销毁、归档、恢复等生命周期管理功能
13		支持 RESTFUL 接口协议，并有统一的接口说明文档，方便第三方应用接入
14		支持密钥状态轮转,支持密钥定时或者手动翻新，翻新密钥名称不变。
15		系统支持 IP 白名单、数字证书、密钥用户和访问口令等方式对客户端进行身份认证。
16		支持为密钥分配密钥用户。

序号	指标细项	指标要求
17	应用密评服务	实现密评机构管理和密码厂商管理，包括新建、删除和编辑功能
18		支持管理密评要求体系管理，包括技术要求和管理要求，支持新建、编辑和删除
19		实现密评要求条目管理，包括密评要求条目的新建、删除、编辑、调研选项管理和改进建议管理的功能
20		支持密评进度模板管理，新建并配置模板信息，包括项目准备、方案编制、改造实施、密码测评部署的具体配置；支持编辑、删除和复制模板。
21		支持密评要求的模板管理，新建并配置模板信息，对具体密评要求进行添加、删除和编辑；支持编辑、删除和复制密评要求模板。
22		支持交付文档模板管理，按制定类型上传和下载交付文档模板，用作指导编写应用密评过程中的文档
23		支持密评应用信息管理，绑定单位、上线和应用服务器管理的功能
24		实现密评对象管理，支持使用密评进度模板和密评要求模板创建密评对象，编制应用的密评流程和密评要求，推进密评进度和密评要求的完成情况，提供根据密评推进情况生成差距分析报告的功能
25		统计展示密评应用总数，应用密评完成数量、密改单位数量、等保级别应用分布、各单位密评完成进度、密评完成趋势等数据

序号	指标细项	指标要求
26		为保障提供的密码系统使用合规性，可提供具有合规检测工具，检测国密国际ZUC、SM4，SM2、RSA、ECDSA、SHA-1、SHA-2 等算法。支持数字证书解析、数字证书链验证和证书验签等。
27		支持知识库管理，动态添加知识库分类，按照分类上传相关文档；支持配置文档访问范围，在线预览 PDF、xls，xlsx，docx，mp4 类型的文档。
28	平台管理功能	★平台应支持多种密码服务功能，至少包括数据加解密服务、签名验签服务、密钥管理服务、安全传输服务、电子签章服务、时间戳服务、协同签名服务、OTP 动态令牌服务、文件加密服务和数据库加密服务。
29		平台支持透传密码设备原生接口，实现原有业务系统保持既有运算逻辑零改造。
30		平台所支持密码服务的底层应都依赖云服务器密码机，即实现密码设备的归一化，无需其他密码设备，从而方便云平台整体对密码设备的统一纳管和后期运维。
31		平台自身满足密评合规的相关要求，包括 1）管理员支持基于智能密码钥匙的“双因子”身份鉴别；2）平台日志和访问控制信息支持基于 HMAC_SM3 完整性保护；3）密码服务接口支持基于 AK/SK 的身份鉴别；4）平台管理端和租户端支持基于国密 SSL 安全隧道的远程管理

序号	指标细项	指标要求
32		平台应支持租户侧和管理侧具备独立的管理界面，租户侧包括租户管理首页可查看当前租户、密钥数量、证书数量、异常服务等内容。管理侧应具备 license 授权管理、租户管理、服务管理、设备管理、用户管理和日志管理等。
33		应支持应用管理，可以针对租户下的每个应用进行应用注册、应用绑定、应用编辑和应用删除等。
34		应支持基于 license 授权的密码服务实例发放，实现密码服务的按需供给。
35		支持对租户端管理界面的操作员实行基于“限时”的登录管制，适用于应用集成商代租户进行密码配置操作的场景，可以限制其登录使用的时长。
36	平台监控功能	监控设备与运行状态及密码资源状况监控、实现服务运行状态实时监控、实现应用系统密码服务调用监控
37		实现异常状态自动告警功能等功能
38		针对密码资源的使用情况定期进行报表
39		支持日志记录功能，包括系统日志、错误日志和操作日志等。
40		支持日志查看及导出功能；
41		日志至少保存 6 个月以上，并可通过 Syslog 进行转发
42	产品资质	★所投产品具备商用密码认证证书，且符合 GM/T 0028《密码模块安全技术要求》

序号	指标细项	指标要求
		第二级要求。
43		支持国产化国产处理器、操作系统、数据库、中间件兼容互认证并分别提供每个类别证明报告；

附件 2：《验收标准》

序号	验收条件	描述	备注
1	设备到货	合同约定货物完成到货验收工作，并提供甲方认可的产品检验合格证明文件、到货单、保修单、用户操作手册、配置文档等。	
2	设备安装调试	产品全部完成安装调试，项目内容全部完成并可以开通使用。	
3	材料齐全	已经提交完整的工作总结报告、安装调试记录及相关文件。	
4	完成试运行	系统试运行期限结束，并提供相应的试运行记录。	
5	验收申请	系统上线后，乙方向甲方提出验收申请 30 工作日内，甲方组织验收工作开展并按照招标文件内容进行项目验收。	

附件 3：

合作伙伴廉政协议

为共同维护商业活动公平竞争秩序，保证双方在业务交往活动中做到诚信、廉洁、高效和共赢，特订本协议如下：

1、双方在合作过程中，自觉遵守国家法律、法规，按照《中华人民共和国反不正当竞争法》、《中华人民共和国招标投标法》、《关于禁止商业贿赂行为的暂行规定》以及其他相关法律规定开展商业交易活动。

2、在供应商资格预审、投标、开标与评标等过程中，做到公平、公正、公开，禁止暗箱操作。甲方监察部门或其授权人员按照规定对招投标项目实施监督，对于乙方有关招投标的投诉和举报，监察部门认真调查，秉公处理，及时回复。

3、双方相关工作人员及其亲属，不得收受对方馈送的现金、贵重物品、有价证券等，不得要求或接受对方为其住房建修、婚丧嫁娶、出国等提供资助，不得介绍亲友从事与双方合作有关的业务活动，不得收受回扣，不得参加影响公正执行公务的高档娱乐、宴请、健身或旅游活动，不得由对方报销应由本人支付的费用。

4、双方相关工作人员不得为谋取私利私下就材料供应、数量变化、材料质量问题处理等进行私下商谈或者达成默契。

5、不做违反商业道德、扰乱正常竞争秩序、有损双方形象的事情，不围标、串标，不泄露双方机密，不排挤其他经营者的公平竞争，不在预决算、招投标和商务报价中弄虚作假或恶意高估冒算。

6、双方人员发现对方人员有受贿或索贿行为以及徇私舞弊、滥用职权、严重渎职等情况时，有义务向对方监察或相应部门举报。

7、乙方若违反廉政协议将被列入廉政黑名单，甲方将视情节轻重，停止该项目或类似项目的合作，一至三年内不再邀请其投标或比选，不再开展新的业务合作。

8、甲方人员若违反廉政协议，造成公司重大损失或恶劣影响的部门和人员，将按照相关规定进行处理，对于涉嫌犯罪的，按照有关程序移送司法机关。

甲方举报渠道	乙方举报渠道
电话：65099922	电话：61842577

附件 4：乙方账户信息

京闽数科（北京）有限公司信息 ：

营业执照注册号：91110105MACGUE9P79

地址：北京市朝阳区望京东路 1 号 2 层 201 内 B202

法定代表人：张春雷

联系电话：010-61842577

账户名称：京闽数科（北京）有限公司

开户银行：中国民生银行股份有限公司东坝支行

公司账号：639924158