海淀区城市治理云平台服务项目合同

项目名称：海淀区城市治理云服务项目

甲　　方：北京市海淀区大数据中心

乙　　方：联通数字科技有限公司

合同编号：

签订地点：北京市海淀区

合同正文

依据《中华人民共和国民法典》以及国家其他有关法律法规的规定，甲、乙双方遵循平等自愿、诚实信用的原则，就乙方向甲方提供海淀区城市治理云平台服务项目事宜经协商达成一致意见，签订本合同，并共同遵守。

第一条 合同各方

甲方：北京市海淀区大数据中心

乙方：联通数字科技有限公司

第二条 合同术语定义、解释和适用范围

2.1 云计算服务：云计算服务是一种处理能力可弹性伸缩的计算服务，其管理方式比物理服务器更简单高效。云服务器帮助用户快速构建更稳定、安全的应用，降低开发运维的难度和整体 IT 成本，使用户能够更专注于核心业务创新。

2.2 海淀区城市治理云：甲方依托乙方提供的基础设施环境、资源以及服务部署专享的云平台，为海淀区政务领域提供云计算服务。

2.3 下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：1.本合同及其变更、补充协议；2.中标通知书；3.投标文件；4.招标文件；5.联合协议/分包意向协议（如有）；6.技术培训方案及售后政策（如有）；7.有关技术文件、图纸（如有）；8.国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件。

第三条 服务内容

本次采购为基于国产技术架构的城市治理云平台服务，云资源应构筑在国产 CPU 和国产操作系统之上，为海淀区提供国产云服务器、云存储、网络接入、国产操作系统、国产中间件、国产数据库、视频结构化分析、智能算力、云资源管理及安全保障服务。云平台按照政务外网业务区和互联网业务区进行安全隔离，并分别提供计算、存储、网络和安全资源池。

3.1 专属机房服务需求

3.1.1 考虑到本项目涉及区政务数据高敏感性与属地化安全管理要求，乙方在北京市海淀区辖区内为甲方提供专属机房空间，机房应符合公安部等保三级标准；

3.1.2 乙方建设的区城市治理云平台应部署在专属机房空间，实现所有计算、存储等设备的物理隔离；

3.1.3 提供实时监控系统，对专属机房空间情况进行实时监控。

3.2 云计算资源服务需求

3.2.1 云服务器 vCPU 数量不少于 4300 核，云服务器内存数量不少于 13700GB，提供按使用量

付费方式；

3.2.2 云服务器提供弹性伸缩及快速横向扩展功能；

3.2.3 基于国产虚拟化软件创建和管理云服务器，提供常见的迁移模式技术支持；

3.2.4 提供国产操作系统、国产中间件；

3.2.5 提供自动化批量部署云服务器能力；

3.2.6 提供云服务器的日常管理操作能力；

3.2.7 云服务器应支持多元计算服务 C86、ARM 两种架构，可由一个或多个云管平台提供服务。

3.3 算力服务需求

3.3.1 提供不少于 256 路等效视频结构化分析算力，服务应覆盖视频解码、结构化分析、任务调度、运行监控和故障处置，并支持按业务需求进行资源分配。

3.3.2 提供 FP16 精度不低于 17.5PFLOPS 的智能算力资源，配套算力管理工具及运维服务，支持资源申请、分配、监控、统计和故障告警。

3.4 云存储资源服务需求

3.4.1 普通性能云存储的存储空间不少于 388350GB,提供按使用量付费方式；

3.4.2 高性能云存储的存储空间不少于 50T，提供按使用量付费方式；

3.5 网络资源服务需求

3.5.1 核心交换机之间采用全网状连接，核心交换机与接入交换机之间支持云服务器分配网络资源，支持云服务器网络划分网段；

3.5.2 提供对多台云服务器进行流量分发的负载均衡服务；

3.5.3 提供云上私有网络，可以在自定义的专有网络中使用云资源；

3.5.4 满足政务外网与互联网的安全隔离要求，提供网关配置功能，实现单向访问控制等需求。

3.5.5 支持 IPv6 地址分配，满足业务系统 IPv6 要求。

3.6 安全服务需求

3.6.1 云平台应建立覆盖网络边界、计算环境、应用系统、安全管理及审计的安全防护体系，满足国家网络安全等级保护 2.0 相关要求，并支持按照项目定级要求开展安全建设、测评及整改。

3.6.2 应提供云平台网络边界访问控制及安全防护能力，支持安全策略配置、入侵防御、恶意流量检测等功能，实现云内不同安全区域及云平台与外部网络之间的安全隔离。

3.6.3 应提供 Web 应用安全防护能力，支持对 SQL 注入、跨站脚本、恶意扫描、网页篡改、CC 攻击等常见 Web 攻击进行检测和防护。

3.6.4 应提供云服务器安全防护能力，支持资产管理、恶意程序检测、漏洞检测、基线检查、入侵检测及 WebShell 检测等功能。

3.6.5 应提供面向云服务器、网络设备及 Web 应用的漏洞扫描能力，支持操作系统漏洞、Web 漏洞、弱口令及配置风险检测，并提供漏洞修复建议。

3.6.6 应提供统一的运维访问入口，支持账号管理、身份认证、权限控制、操作审计、命令审计及运维过程回放等功能。

3.6.7 应支持对云平台、云服务器、网络设备、安全设备的日志进行统一采集、集中存储、查询分析和审计，并支持安全事件告警及审计报表生成。

3.6.8 应提供数据库访问行为审计能力，支持数据库访问记录、操作行为分析、风险行为识别、异常操作告警及审计报表生成。

3.7 资源管理和安全保障服务

3.7.1 资源管理服务

3.7.1.1 提供日常运维、故障处置、问题排查、技术支撑等现场服务工作，提供每周 7 天×24 小时响应服务，保障业务系统持续稳定运行。

3.7.1.2 提供云资源、网络资源及安全策略的配置管理服务；

3.7.1.3 提供系统入云部署及云资源使用等方面的技术支持，包括资源开通、管理、监测、配置、故障处理、应急处置等；

3.7.1.4 提供入云系统运行监测及云资源使用优化服务，每周对云资源使用情况进行统计分析，制定资源优化方案及计划，提升云资源使用率；

3.7.1.5 提供网络安全监测、分析、处置服务，对入云系统安全策略及网络安全事件提出处置建议和优化方案；

3.7.1.6 提供云资源管理及入云系统安全监测运维周报。

3.7.2 安全保障服务

3.7.2.1 提供满足国家等保三级防护标准、以及国家密码应用建设的区城市治理云平台安全防护体系；

3.7.2.2 提供可靠的安全保障服务，包括但不限于出口防护、运维安全管控和审计等服务。

3.7.2.3 提供云平台及入云系统整体漏扫服务，每季度至少开展一次，涵盖云平台上的所有关键组件和服务。

3.7.3 国产化适配服务

需配合各单位业务系统进行国产云迁移适配，沟通国产资源需求和软件需求，解决业务系统适配问题。

3.7.4 重保服务

提供重要时期安全保障服务，在国家重要节日、重大活动、重要会议等关键时期，采取安全保障措施保障信息安全。

第四条 技术要求

4.1 基本服务要求

4.1.1 本次云服务使用的 CPU、操作系统、中间件、数据库均为国产产品。

4.1.2 云平台产品为正式版商用产品，保障后续产品的连续性。

4.1.3 云平台应提供功能完整的服务能力，如云服务器、存储、云数据库、云中间件、云网络等服务产品。

4.1.4 云平台所提供的云服务器产品，当云服务器现有配置不满足要求时,用户可自主进行云服务器配置快速升级，可升级配置包括：CPU、内存、数据盘大小等。

4.1.5 网络接入需要提供互联网跨运营商访问优化技术服务能力。

4.1.6 云平台应支持符合国家密码管理要求的商用密码算法，包括 SM2、SM3、SM4 等，并按照现行密码应用相关标准规范进行建设，满足网络安全等级保护第三级及商用密码应用安全性评估要求。

4.1.7 本项目涉及区政务数据安全与属地化管理要求，所提供的云服务由私有云平台提供，不接受公有云形式，云平台的网络划分为政务外网区和互联网区两个区域，其中政务外网区和互联网区安全隔离，通过跨网安全隔离交换系统实现两个区域间数据安全交换。

4.2 计算服务要求

4.2.1 云服务器支持丰富的国产操作系统类型，兼容主流国产化操作系统，至少包括大于三种国产操作系统。

4.2.2 支持申请云服务器时自定义开机执行的命令、脚本或注入文件。

4.2.3 支持云服务器设备直通，用户申请云服务器时，可以申请将 GPU、SSD 磁盘等设备映射给云服务器使用。

4.2.4 支持云服务器整机快照，保障包括系统盘和多块数据盘之间的崩溃一致性，避免单个盘快照导致系统数据不一致。

4.2.5 支持云服务器或云服务器所在主机故障，系统会自动在其他主机上重建云服务器，保证业务的连续性。

4.2.6 支持云服务器监控管理，提供性能监测分析、异常告警等功能，支持监控指标包括 CPU 使用率、内存使用率、网络流入/流出速率、云硬盘 IO 速率、GPU 利用率等。

4.2.7 支持租户删除云服务器时放入回收站，并支持从回收站恢复云服务器，防止误删除导致数据丢失和业务中断。

4.2.8 云服务器镜像支持除了支持公共镜像、私有镜像以外，还支持共享镜像方式，即用户可以将自己的私有镜像共享给其他特定的用户使用。

4.2.9 支持数据盘镜像，支持在租户界面通过云服务器数据盘制作数据盘镜像；使用数据盘镜像可以创建云磁盘；数据盘镜像支持导入导出操作。

4.3 网络服务要求

4.3.1 为保障网络扩展性、可靠性和硬件解耦，要求本次 SDN 网络相关软件网元，包括虚拟路由器、虚拟交换机、负载均衡等，应采用软件方式部署，不依赖特定硬件设备实现。

4.3.2 支持 VPC 添加多段地址空间，支持在地址扩容场景添加容器或者 IaaS 扩展地址空间，一个 VPC 支持添加一个主网段和扩展网段。

4.3.3 因云服务在应用中大量涉及跨节点数据传输，VPC 须支持组播能力，支持通过图形化界面配置组播开启、关闭操作。

4.3.4 支持为云服务器在线添加网卡并设置 IP 地址，支持单台云服务器配置多个网卡。

4.3.5 支持 VPC 拓扑，支持图形化拓扑展示当前 VPC 的子网信息，以及使用该子网的云服务信息。

4.3.6 支持安全组服务，可以对进出云服务器端口的网络报文进行安全过滤规则设置。云服务器端口与安全组关联后，安全组规则可对进出云服务器端口的网络报文进行过滤，只有规则允许的报文可通过。

4.3.7 支持安全组规则的导入、导出操作。

4.3.8 支持安全组绑定到不同 VPC 的云服务器，支持关联安全组到辅助网卡。

4.3.9 支持负载均衡服务，负载均衡服务基于软件方式实现，不依赖于特殊硬件设备。可以将用户业务访问流量自动分发到多台云服务器，扩展应用系统对外服务能力。

4.3.10 支持跨 region 网络互通能力，可以实现多个 region 间 VPC 网络自动化互通能力。用户可在管理界面上进行跨云连接服务的创建，修改和删除。

4.4 存储服务要求

4.4.1 支持云硬盘服务，用户可以通过管理平台为云服务器申请磁盘，用户可以将申请到的磁盘空间分配给云服务器使用，支持云硬盘进行在线/离线扩容。

4.4.2 支持云磁盘的新建、扩容、挂载、卸载、申请快照、重命名、删除、变更类型等基本操作。

4.4.3 支持云硬盘的管理，用户可以查看系统中已有的硬盘列表，可以查看磁盘名称、状态、容量、挂载到的服务器、创建时间等基本信息；支持快速搜索磁盘，可以通过磁盘名称或者磁盘是否挂载等条件搜索目标磁盘/磁盘组。

4.4.4 支持快照服务，用户可以通过管理平台为自己的云服务器/云服务器磁盘/裸机磁盘创建快照，单磁盘支持多个快照，支持自助完成快照恢复。

4.4.5 支持系统盘和数据盘在线扩容，扩容不中断业务。

4.4.6 支持对象上传、下载、删除、查询、共享，支持对象多版本，支持存储话单，支持桶的配额设置和查询，支持创建桶、删除桶，查询所有桶，设置桶内对象的生命周期，支持 HTTPS 访问。

4.4.7 支持两个对象存储集群间的数据复制，提高数据可靠性。

4.4.8 支持对桶配置默认服务端加密功能，配置后，上传到桶中的对象都会自动进行加密。

4.5 云管服务要求

4.5.1 支持通过图形化界面对云服务进行编排，可视化编排界面支持任意拖拽图元，快速完成云服务器、裸机、容器、弹性伸缩、存储、网络等资源的组合编排和自动化部署，支撑业务快速上线。

4.5.2 支持按操作授权，包括按组织、服务、应用、计量、审批等操作进行精细化授权控制。

4.5.3 支持用户的创建、删除、修改、查询、禁用、重置密码等操作，并可限定每个用户操作的资源范围。

4.5.4 支持通过计量计价可以统计各部门的资源使用情况、费用使用。支持核算各部门的资源使用量是否超过预算。支持按小时/天/月设置单价满足客户按需结算要求。

4.5.5 支持统一资源管理，包括各类云资源、脚本资源、软件资源，支持查看已分配资源和资源回收站，支持通过资源中心快速的管理在云平台上申请的资源，支持按照多种维度查看资源。

4.5.6 支持用户删除资源后保留到回收站，允许误删除后恢复资源。支持回收站的资源包括云服务器、云磁盘、数据库服务等。

4.5.7 云平台具备统一运维管理能力，提供集中监控、资源拓扑、日常运维、运维分析、系统管理等能力，实现物理设备到应用的全方位监控，收集并展示运维对象的告警、日志等信息，同时提供报表、大屏、自动化以及高级运维数据分析能力，简化日常运维工作，提升运维效率。

4.5.8 支持对各区域资源的告警、性能指标等进行全方位监控，及时了解资源运行状态，当发生告警时快速通过页面、短信、邮件等方式通知相关人员，对故障进行定位定界，提高运维效率。

4.5.9 支持对云平台各类管理数据的自动备份，支持升级业务或重大业务调整前，对系统数据进行手动备份，保证系统在出现异常情况时，能够快速恢复数据并稳定运行。

4.6 云安全服务要求

4.6.1 乙方所投主机安全、堡垒机、云防火墙、数据库审计等核心云安全产品，支持与所投云平台深度融合，所投云平台同一套账号体系。支持在云管理平台直接使用管理安全能力；支持对安全产品及服务进行统一管理，包括统计用量，使用情况监控。

4.6.2 乙方所投云平台应满足通过网络安全等级保护三级的能力要求。

4.6.3 乙方所投云平台应满足通过商用密码应用安全性评估三级的能力要求。

4.7 国产操作系统服务要求

4.7.1 中文支持：提供中文输入法支持。

4.7.2 文件系统支持：至少支持 Ext3、Ext4、XFS 等文件系统。

4.7.3 提供 Apache http、ftp、DNS、DHCP、NFS、Samba、LDAP 等应用。

4.8 国产中间件服务要求

4.8.1 支持云服务器、物理机、容器环境部署，支持轻量版本和 springboot 环境使用版本。

4.8.2 支持多服务器集群部署、负载均衡，支持 Web 层的集群和 EJB 集群。

4.8.3 提供完善的集群技术与 Session 管理，支持 Session 数据配置接入分布式缓存如 Redis 集群等,实现 Session 数据的独立管理。

4.8.4 支持组件级的失效即时恢复（Fail Over）。

4.8.5 提供多数据源功能,支持将多个普通数据源配置成多数据源。

4.8.6 支持通过界面进行补丁升级、回退功能。

4.9 国产数据库服务要求

4.9.1 支持 ANSI SQL-2003 以上标准；支持 JDBC/ODBC 标准接口。

4.9.2 支持逻辑备份恢复、物理备份恢复，物理备份支持增量备份、联机热备份、备份压缩等技术。

4.9.3 支持 HA 故障转移集群和主备同步技术，并且能够支持读写分离以及故障转移功能，支持主从、一主多从。

4.9.4 支持自主访问控制、基于安全标签的强制访问控制、用户角色三权分立、审计、加密、身份识别与验证等安全功能。

4.9.5 支持系统性能监控动态视图，TOP SQL 信息、内存管理信息、事务信息、线程信息、操作历史等信息。

4.9.6 支持通信和存储加密功能，支持库级别的磁盘文件级加密，支持国密算法。

第五条 计费方式及支付方式

5.1 计费方式

本项目为按照甲方需求以购买服务的方式向乙方购买相关服务，并根据实际购买服务结算费用。

5.1.1 甲方购买服务应按照《服务内容及价格表》（见附件 1）内约定服务内容进行购买，如有其他服务需求，需签订补充协议补充服务内容后再购买。

5.1.2 甲方购买服务的期限不能超过本合同服务期限。

5.1.3 结合以上 5.1.1、5.1.2 条款内容，以甲方最终在本合同服务期内实际使用的服务内容及数量，依据本合同服务期约定的《服务内容及价格表》（见附件 1）进行本合同服务期计费计算。

5.2 支付方式

本项目价款以人民币结算，预估合同总价款为人民币 17,111,076.00 元（大写：壹仟柒佰壹拾壹万壹仟零柒拾陆元整），具体结算金额以财政实际批复为准。根据城市治理云所需要的计算资源和存储资源的实际使用量进行结算。

5.2.1 第一笔款：自服务期开始之日起 6 个月内，甲方收到乙方提供的发票后 10 个工作日内，向乙方支付预估合同总价款的 50%，即服务费￥8,555,538.00 元（大写：人民币捌佰伍拾伍万伍仟伍佰叁拾捌元整）。

5.2.2 尾款：服务期结束后 60 个工作日内，乙方提供甲方本合同服务期服务费用说明（以本合同 5.1 计费方式条款约定的计费方式计算得出），甲方核实后结算本合同服务期剩余服务费。

5.2.3 合同执行过程中，乙方应按月提供每月实际使用费用账单，如出现本合同服务期服务费用超过本项目预算资金的趋势，乙方应及时提示甲方追加预算。

5.2.4 本合同项下服务费用原则上不得超过本项目经批准的预算金额。未经甲方事先书面确认并履行相应预算审批、合同变更等程序，乙方不得擅自提供超出预算范围的服务，甲方亦无义务支付未经书面确认的超预算费用。确需追加服务内容或预算的，由双方另行协商并依法履行相关程序。

5.2.5 本合同最终结算金额以甲方审核及第三方审计结果（如有）为准；如甲方已付款金额超过最终审定金额，乙方应在收到甲方通知后 10 个工作日内返还差额。

5.2.6 乙方知晓甲方支付款项来源于财政拨款，若因财政拨款未及时到账导致甲方付款延迟的，付款时间自动顺延，具体付款时间以财政资金到账时间为准。顺延期间，甲方不承担违约责任。

5.2.7 甲方付款前，乙方应向甲方提供等额、合法、有效的增值税普通发票。因乙方未及时提供发票或者发票有问题，甲方可延迟付款，相应责任由乙方承担，甲方不承担违约责任。

第六条 交付工期及验收

6.1 交付期

6.1.1 乙方在签订合同后 60 个工作日内完成合同规定的区城市治理云搭建和部署，满足业务上线要求。

6.1.2 乙方完成区城市治理云搭建和部署，并通过测试验收后，开始计算服务期，服务期为期一年。在服务期中，乙方需根据服务需求提供相应的资源服务。

6.2 验收

6.2.1 甲方在签订合同后 60 个工作日内对乙方提供的城市治理云服务进行测试，测试通过即为验收合格。

6.2.2 如乙方提供的区城市治理云服务未达到项目招标要求，无法通过测试，甲方有权终止项目执行，并重新进行招标。

第七条 双方权利和义务

7.1 甲方的权利和义务

7.1.1 合同执行期间，区城市治理云使用的基础 IT 资源所有权归乙方所有，城市治理云服务资源使用流程由乙方根据甲方要求统一制定，城市治理云服务资源使用权归甲方所有，区城市治理云上的相关数据所有权归甲方所有。

7.1.2 甲方委托乙方利用城市治理云服务资源为全区政务办公等领域信息系统提供基础 IT 资源支撑和统一规范服务管理。所有经甲方批准部署在区城市治理云的信息系统，如涉及乙方提供的第三方软件许可使用，甲方同意遵守相关许可协议的约束；所有经甲方批准部署在区城市治理云的信息系统，甲方负责协调相关使用单位自行解决云服务器上所需要的非乙方提供的软件版权（许可/使用权），并负责数据的完整性和保密性；甲方负责协调相关使用单位不在区城市治理云上安装、使用盗版软件，并支持乙方拒绝对使用盗版软件的相关使用单位信息系统在区城市治理云上部署。若乙方侵犯第三方权利，由乙方自行处理。

7.1.3 甲方应明确要求全区政务办公等领域相关单位用户对于部署在区城市治理云上的信息系统声明内容责任自负，如内容中有违反政策法规的情况，由业务所有方承担全部责任。

7.1.4 甲方应按时向乙方缴纳本合同约定的费用。

7.1.5 安全措施需由甲方和乙方共同分担，其中甲方负责自己部署的操作系统、运行环境和应用的安全，乙方负责云平台及底层资源的安全。

7.2 乙方的权利和义务

7.2.1 乙方应按照合同约定为甲方提供服务。

7.2.2 乙方对云服务器进行日常维护和监控，以保证其正常运行。

7.2.3 乙方负责提供操作系统，并提供网络环境及城市治理云安全服务。

7.2.4 乙方为甲方提供每周 7 天×24 小时售后服务，并为甲方提供有效的联系方式。

7.2.5 乙方应严格遵守保密义务，除非双方另有书面约定，乙方承认甲方存放在区城市治理云上的任何资料、软件、数据等的知识产权均与乙方无关，乙方无权复制、传播、转让、允许或提供他人使用这些资源。

7.2.6 如服务出现任何问题，乙方应优先协调各方资源处理解决，不推卸、推诿。

7.2.7 如果第三方机构或个人对甲方提出质疑或投诉，乙方将通知甲方，甲方有责任在 5 个工作日内进行说明并出具证明材料，如甲方未能提供相反证据或逾期未能反馈的，乙方在事先通知甲方情况下，可采取包括但不限于立即终止服务、中止服务或删除相应信息等处理措施。因甲方未及时更新联系方式或联系方式不正确而致使未能联系到甲方的，亦视为甲方逾期未能反馈。

7.2.8 因不可抗力因素和甲方原因，造成服务的正常工作中断，乙方不承担责任。

7.2.9 根据甲方需要，在满足乙方技术环境的前提下，乙方应积极配合甲方及其委托的第三方对甲方购买的云服务进行安全审查工作；

7.2.10 云计算服务之间的交互而引起的网络流量属于乙方提供的服务范畴。

7.2.11 在未取得甲方同意的情况下，乙方不得通过任何手段收集、分析、处理、篡改区城市治理云中的数据。禁止数据以任何方式渠道泄露出去。

7.2.12 乙方不得私自将未经甲方审核的系统部署在区城市治理云。

第八条 违约责任

8.1 甲乙双方任何一方不履行合同义务或者履行合同义务不符合本合同约定的，均视为违约。守约方可向违约方发出要求其履行合同义务的书面通知，违约方应在通知发出之日起 5 个工作日内采取补救措施，逾期仍未采取措施的，则守约方有权单方解除本合同或要求违约方继续履行合同义务并赔偿因此造成的损失。

8.2 甲乙双方在完成双方签署的书面确认事项后，任何一方提出变更要求，导致项目进度延迟的，不视为对方违约。

8.3 因甲乙双方任何一方的原因致使另一方遭受第三方追诉的，违约方应赔偿由此给另一方造成的损失。

8.4 因甲方的原因或与甲方具有协作关系的第三方的原因导致项目进度延迟的，乙方不承担违约责任，因此而给乙方增加工作量的，甲方应按照双方协商一致的确认结果给予补偿。

8.5 乙方提供服务过程中可能发生的违约行为及应承担的违约责任见附件：违约行为处罚细则。违约罚款均以人民币结算。

第九条 知识产权及保密

9.1 除以下第九条第 9.2 款另有规定外，甲方和乙方应当各自就其或其雇员、承包商、顾问或代理人获得的关于本合同及本项目（无论是财务上、技术上或其他方面）的全部信息和文件，予以保密。

9.2 以上第九条第 9.1 款不适用于：

9.2.1 已经公布的或能以其他方式公开获得的信息或文件（但不包括以违反本合同的方式公布或获得者）。

9.2.2 已经由一方以不违反任何保密义务的方式获得的信息或文件。

9.2.3 以不违反任何保密义务的方式从第三方获得的信息或文件。

9.2.4 按照法律须披露的信息或文件。

9.2.5 为按照本合同履行一方义务而披露的信息或文件。

9.3 以上第九条第 9.1 款在本合同届满或终止后的十年内仍然有效。甲乙双方对彼此之间相互提供的信息、资料以及本合同的具体内容负有保密责任。

第十条 甲方数据的保存、销毁与迁移

10.1 根据法律有关规定或者行政、司法机构的要求，经甲方同意，乙方可以向第三方或者行政、司法机构提供数据审查。

10.2 除法定及甲乙另行约定外，自本合同服务期满或因任何原因导致本合同提前终止之日起的 60 日内，乙方应继续存储甲方的数据。逾期乙方将不再保留甲方数据，甲方需自行承担其数据被销毁后引发的一切后果。

10.3 甲方要求删除数据或设备在弃置、转售前，乙方需将其所有数据彻底删除，并无法复原。

10.4 乙方承诺甲方启用或弃用云服务时将配合甲方完成数据的迁入和迁出。

第十一条 不可抗力

11.1 本合同中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

11.2 如发生不可抗力，以至于任何一方因这种事件的发生而无法履行或无法完全履行其义务，一方对另一方因此而造成的损失不承担责任。但在不可抗力发生期间及结束之后，在合同的履行仍有意义时，受影响的一方仍应在可能的范围内履行己方的义务，以尽可能减少损失的发生。

11.3 遇有上述不可抗力事件的一方，应在可能的时候立即将事件情况通知对方，并在该事件发生后 15 日内向对方提供政府部门开具的有效证明文件，同时提出合同需要延期履行或不能完全履行或不能履行的理由。按照该事件对合同履行的影响程度，由双方友好协商决定继续履行合同或终止合同。

11.4 一方迟延履行后发生不可抗力的，仍应承担违约责任。按本合同第八条 “违约责任” 约定执行。

第十二条 合同变更

12.1 因项目需求发生变化，需要对合同内容进行变更的，需经双方书面确认。

第十三条 争议解决

13.1 因履行本合同或与本合同有关的一切争议，双方当事人应通过友好协商方式解决，若发生争议协商未成，双方约定由合同签署地有管辖权的人民法院提起诉讼。除非生效裁判另有规定，各方为解决争议而实际支付的费用（包括但不限于诉讼费、保全费、评估费、拍卖费、执行费、合理的律师费等）由诉讼请求未被支持的一方承担。

13.2 在诉讼过程中，除各方有争议的部分外，本合同其他部分继续有效。

第十四条 服务期限与终止

14.1 本合同自双方法定代表人或授权代表签字（签章）并加盖单位公章或合同专用章之日起生效，双方履行完合同规定的义务后自行终止。合同服务期为 1 年，从 2026 年 11 月 1 日至 2027 年 10 月 31 日止。

14.2 服务费用按年结算，第一年服务期结束后，在不改变合同其他条款的情况下，甲方可视服务情况与乙方续签合同，续签次数不得超过两次，总服务期限不得超过三年。本合同为第一年服务期合同。

14.3 发生下列情形，服务期限提前终止：

14.3.1 双方协商一致提前终止的。

14.3.2 甲乙任何一方单方面提出终止合同，需提前三个月通知对方，双方协商解决。

14.3.3 甲乙任何一方违反本合同条款的，包括但不限于未按照合同约定履行付款义务或严重违反法律规定等。

第十五条 合同份数及附件

本合同正本一式 拾壹 份，具有同等法律效力。甲方执 陆 份，乙方执 肆 份，海淀区政府采购中心执壹份。附件系合同组成部分，与合同正文具体同等法律效力。

附件：1.服务内容及价格表；

2.乙方服务要求及违约行为处罚细则

合同签署页

甲方	单位名称	北京市海淀区大数据中心（盖章）
	法定代表人（或授权代表）	签字（签章）：
	项目负责人	卢诚
	电　　话	87130833
	传　　真	/
	邮政编码	100081
	地　　址	北京市海淀区中关村南大街 5 号海淀科技大厦
	纳税人识别号	12110108MB09868857
乙方	单位名称	联通数字科技有限公司（盖章）
	法定代表人（或授权代表）	签字（签章）：
	项目负责人	钟昕
	电　　话	18618152655
	传　　真	010-66504934
	开户银行	中国工商银行股份有限公司北京灵境支行
	账　　号	0200013319200042469
	邮政编码	100035
	地　　址	北京市西城区西单北大街 133 号
签署日期		2016 年 10 月 30 日

附件 1.服务内容及价格表

序号	预算大类	预算小类	费用项	说明	规格	价格单位	单位	需求量	单价（元/月）	服务费小计（元/年）
一	资源管理和安全保障服务	资源管理和安全保障服务	资源管理和安全保障服务包括资源管理服务，安全保障服务，国产化迁移服务及重保服务。				套	1	199500	2394000
二	网络资源服务	互联网	互联网租用服务		1Mbps	元/月	条	2000	38	912000
三	国产云资源服务	云服务器	国产 vCPU	按使用量计费	1 核	元/月	核	4300	14	722400
			内存	按使用量计费	1GB	元/月	GB	13700	36	5918400
		算力服务	视频结构化算力	按使用量计费	1 路	元/月	路	256	182	559104
			智能算力服务	按使用量计费	1PFLOPS	元/月	PFLOPS	17.5	18671.5	3921015
		云存储	普通存储	按使用量计费	1GB	元/月	GB	388350	0.285	1328157
			高性能存储	按使用量计费	1TB	元/月	T	50	600	360000
		操作系统	国产操作系统	按使用量计费	套	元/月	套	520	48	299520
		数据库	国产数据库	按使用量计费	套	元/月	套	204	250	612000
		中间件	国产中间件	按使用量计费	套	元/月	套	80	88	84480
合计										17111076
注：需求量为预估值，甲方有权按照资源实际使用情况进行调整，费用按照实际资源使用量核算。										

附件 2.乙方服务要求及违约行为处罚细则

第一条 乙方提供的服务要求

1.1 为保障上云系统的正常运行，乙方每天应进行 2 次城市治理云健康检查，检查内容包括但不限于城市治理云控制节点、计算节点、存储节点、数据库集群，并将检查报告通报甲方。

1.2 乙方应对检查过程中发现的城市治理云软硬件风险隐患进行修复维护；在维护操作前，乙方应向甲方提交实施方案，说明处置流程和处置人员，经甲方批准后，严格按方案实施操作，操作完成后向甲方通报结果，并记录备案。

1.3 乙方进行城市治理云系统版本迭代前，应向甲方提交风险评估报告和测试报告，确保甲方信息系统在不同版本环境下均可稳定运行。

1.4 乙方应根据甲方信息系统上云计划，提前进行城市治理云扩容所需物理服务器、网络设备、互联网带宽等资源的部署，并保证城市治理云可用资源冗余不少于现有资源的 20%。

1.5 乙方应根据国家互联网应急中心公布的威胁预警情报对城市治理云上的系统和软件进行全面的漏洞扫描与病毒查杀，发现问题应及时进行处置并通报甲方。

1.6 乙方应持续优化城市治理云安全组策略和防火墙入站规则，加强城市治理云的安全访问控制策略，形成双重保险机制。

1.7 乙方应持续升级完善城市治理云安全防护系统，加强城市治理云用户侧的安全防护功能；对涉及民生、政务等重要信息系统应进行重点防护。

1.8 乙方接到甲方故障通报后，应及时处理，做好相关信息的登记工作，定时向甲方反馈处置进度及结果；故障排除后，乙方应向甲方提交故障发生及处置过程中全部软硬件日志和故障分析报告，明确故障原因和整改措施，并严格落实整改措施，杜绝类似故障再次发生。

1.9 乙方应确保城市治理云运维人员符合岗位要求，运维人员到岗前，需经过全面系统的技术培训、安全培训、保密事项培训。

1.10 乙方应确保城市治理云运维团队稳定，运维人员变动需提前一个月通知甲方。

第二条 乙方违约处罚细则

乙方服务期内未能达到合同及附件的约定的服务标准，发生违约行为，甲方将按相应违约行为进行处罚。违约行为分为重大违约行为、严重违约行为和一般违约行为。

2.1 乙方重大违约行为

乙方服务期内的违约行为造成城市治理云整体故障（非不可抗拒力条件下）或重大安全事故的（根据其严重程度分为 A 级事件和 B 级事件）。乙方触发该 A 级事件或一年内三次及以上 B 级事件违约行为，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

一年内 B 级事件发生少于三次，罚款金额=当月城市治理云服务费*30%。

类别	范围	影响	影响时间	事件级别	次数

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（乙方主责）	服务中断	城市治理云整体	因非不可抗力造成超过30%以上业务系统中断、影响人数50万以上、导致500万元以上经济损失。	2小时以上	A级	1次
	重大篡改事件	应用系统	在重大或特别重大保障期间，因乙方的安全隐患原因造成的系统被恶意篡改事件。事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、市级领导批示或关注的。	30分钟以上		
	数据丢失	等保三级或重要业务系统的核心业务数据	因非不可抗力造成的城市治理云超过3个业务系统丢失超过1个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要业务系统	被第三方安全机构通报城市治理云存在安全隐患，乙方未在24小时内做有效处置或应急防护措施，造成业务系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	城市治理云整体	因非不可抗力造成超过10%至30%业务系统中断、影响人数10万以上、导致100万元以上经济损失。	2小时以上	B级	一年内3次以上
	重大篡改事件	应用系统	因乙方的安全隐患原因造成的系统被恶意篡改事件，事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误，且该事件被市级机构或媒体通报、区领导批示或关注的。	30分钟以上		
	数据丢失	业务系统核心业务数据	因非不可抗力造成1个业务系统丢失超过1个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	业务系统	被第三方安全机构通报城市治理云存在安全隐患，乙方未在24小时内做有效处置或应急防护措施，造成业务系统被恶意篡改或敏感信息泄	——		

类别		范围	影响	影响时间	事件级别	次数
			露事件。			

2.2 乙方严重违约行为

乙方在服务期内的违约行为对用户业务系统产生一定的经济损失，但其影响和经济损失未达到重大违约行为中规定的 B 级事件的。

罚款金额=业务系统所使用的云资源服务费/服务月数*惩罚系数。

序号	问题描述	惩罚系数
1	所提供的云服务器可用性低于 99.95%，数据可用性低于 99.999%，网络可用性低于 99.99%，出现问题并造成重大损失的	200%
2	因未做好系统和数据互备，由于城市治理云服务中断，而导致系统和数据无法正常应用的，但影响未达到 B 级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在甲方已发出整改通知后未正确处置，出现问题并造成重大事故	200%

2.3 乙方一般违约行为

乙方在服务期的违约行为对用户业务系统造成的影响未达到重大违约行为和严重违约行为的其他违约行为。

罚款金额=业务系统所使用的云资源服务费/服务月数*惩罚系数。

序号	问题描述	惩罚系数
1	所提供的云服务器可用性低于 99.95%，数据可用性低于 99.999%，网络可用性低于 99.99%，出现问题但未造成重大损失的	50%
2	所提供的云服务器可用性低于 99.95%，或数据可用性低于 99.999%，网络可用性低于 99.99%，且在服务期内接到委办局投诉此类情况 3 次以上的	20%
3	在运维期间，甲方对乙方实施月度考核，如乙方连续 3 次未能通过考核，经限期整改后仍不能达到甲方要求的	20%
4	在运维期内，如乙方未能按照用户方的扩容需求，在 14 个自然日内完成城市治理云的资源扩容，且经管理单位书面通知仍未能限期满足用户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机 2 小时以上	30%
6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机 3 次以上或累计 8 小时以上	60%
7	在甲方已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%