2026年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统

项目合同

合同编号： FW2026082001

甲　　方：北京市城市运行管理事务中心

乙　　方：中国联合网络通信有限公司北京市分公司

根据《中华人民共和国民法典》及其它相关法律法规的有关规定，甲乙双方为明确彼此的权利和义务，经协商一致，共同签订本合同。

下列文件构成本合同的组成部分，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、甲乙双方签订的补充协议（如有）

2、本合同书

3、中标通知书

4、投标文件

5、招标文件

第一条　项目角色定义

1、合同甲方：北京市城市运行管理事务中心

2、合同乙方：中国联合网络通信有限公司北京市分公司

3、政务云管理单位：北京市政务服务和数据管理局

4、云综合监管服务商：经政务云管理单位授权，开展政务云安全、技术监督管理和服务评价的单位

第二条　项目内容

1、乙方应按照《北京市市级政务云管理办法》的有关规定，对甲方如下信息系统提供政务云运行环境开展云租用工作。

序号	信息系统名称
1	北京市能源运行综合监测系统
2	北京市能源运行综合监测系统-感知
3	北京市城市运行监测系统
4	北京市建筑垃圾车辆运输管理系统

2、本合同履行期限内，乙方向甲方提供如下云服务或云资源租用服务。

（1）政务云租用云计算资源清单

服务类别	服务子类	服务项	单位	数量

计算服务	平台云主机服务（包含 X86、ARM、C86）	vCPU（vCPU ARM 架构主频不低于 2.4GHz，C86 和 x86 主频不低于 2.2GHz，平均虚拟化率，即物理 CPU/虚拟 CPU≥1/4，虚拟 CPU 利用率不低于物理 CPU 的 25% ）	1CPU/月	824
		内存	1GB/月	3016
	物理服务器租用服务（包含 X86、ARM、C86）	物理服务器配置 2：四路每 CPU 核数≥48 核，主频≥2.6Ghz，256G 内存，2 块 600G SAS 硬盘，2 个 HBA 卡，2 个万兆端口	1 台/月	6
存储服务	普通性能存储	普通存储（单盘技术指标：单盘 IOPS 2000-5000）业务所使用存储	100GB/月	734.88
	高性能存储	高性能存储（单盘技术指标：单盘 IOPS 10000-25000）	100GB/月	784.88
	本地备份服务	通过备份策略实现文件、操作系统、数据库的本地备份（不包含备份存储空间）	100GB/月	339.04
网络服务	互联网链路服务	互联网链路带宽、提供多线运行商接入服务，保证稳定可靠	1 Mb/月	500
		提供互联网地址租用，并提供网站域名备案服务	1 IP/月	2
	主机负载均衡服务	提供主机应用集群负载均衡服务	1 IP（内网）/月）	7
	远程接入服务	每个账号结合身份验证通过 VPN 远程接入堡垒机进行维护	1 账号/月	7
	VPN 接入服务	用户通过 SSL VPN 访问业务系统	1 套/月	8
	SSL 证书	为网站提供 https 保护，对流量进行加密，防止数据被窃取	1 域名/月	8
	Web 应用防火墙（WAF）	针对网站及 Web 应用系统提供应用层安全防护，支持各类 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护（200Mbps）	1 套/月	7

（2）政务云租用扩展资源清单

服务	服务子类	服务项	单位	数量

类别				
基础软件支撑服务	国产操作系统套餐	麒麟 v10 操作系统服务租用、安装及维护	1 个云主机/月	65
安全监测及防护服务	主机杀毒服务	对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响	1 台/月	65
	主机防护	提供符合等保三级要求的主机权限管理及安全防护	1 台/月	65
	主机安全加固	针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞	1 台次	130
	网页防篡改服务	通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性	1 监控点/月	6
	主机漏洞扫描	为用户提供针对主机层面的安全扫描服务，并反馈相关结果	1 台次	130
	主机日志分析	针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况	1 台次	260
	数据库审计服务	支持 Oracle、SQL-Server、DB2、MySQL 等数据库审计（1 套为 1 个数据库实例）	1 套/月	12
	云端 APT 防护服务	针对高级持续性威胁（APT）提供威胁情报收集、检测和响应的安全防护服务	1 套/月	1
其他服务	云防护系统	云防护、CC 防护、独享 DoS 防护、流量包、重保只读、爬虫防护、威胁情报联动、Web 漏洞扫描、可视化大屏、国密证书、API 安全防护、数据安全、日志服务	1 域名/年	3

	资产测绘与攻击面管理系统	为每个域名提供 20 个 IP/子域名攻击面检测服务；资产发现；资产管理、资产关系；Web 风险扫描；高危端口识别、端口风险扫描；弱口令识别;主机风险扫描；风险/漏洞管理；规则库持续更新;每季度提供一次 ASM 的资产清查和风险检测报告	1 域名/年	3
	专家服务	提供专家服务，包括产品配置、策略优化；7*24 小时电话支持服务、远程技术支持：包含防护接入、防护过程中的问题支持；7*24 小时网站安全监测，网站内容监测、网站可用性监测，威胁情报工单受理，下发，威胁事件协助排查	1 域名/年	3

（3）基础安全保障服务清单

服务类别	服务目录	服务项
安全管理服务	运维人员管理	7x24 小时运维人员管理、安全登记
	机房运维管理	机房设备管理、安全控制
	应急演练	协助使用单位进行安全应急演练
安全技术服务	物理访问控制	机房进出控制、监控等
	机房三防服务	机房防火、防盗、防雷电
	设备访问审计	设备访问记录、日志统计、安全事件
	出口流量监测	出口流量控制、检测，并且可观测数据，互联网网络行为审计
	本地抗 DDoS 防护	云平台整体提供总带宽为 20Gb 的抗 DDoS 防护
	防火墙安全防护	出口安全
	防入侵监测 IPS	防入侵监测
	远程接入服务	提供 1 个远程登录堡垒机的运维账号
	租户隔离	租户虚拟化层隔离
	租户内部访问控制	租户内部访问权限控制，用户可以自由分配
	云主机监控	提供云上资源的基本监控，包括 CPU、内存使用率等

	角色权限管理	提供通过代入角色实现获取操作权限
	监控平台接入服务	可提供租户管辖内的云资源监控数据接口调用
	数据传输服务	在安全隔离的基础上，实现精细控制数据流向，提供不同级别网络间安全可控的请求转发或数据摆渡，确保数据的机密性、完整性和可用性。

第三条　技术水平

1、乙方应为甲方提供本合同约定的全部项目内容，协助甲方开展信息系统部署迁移工作，作好云主机等云资源或云服务的运维工作。

2、乙方为甲方提供的技术支持和成果质量应符合国家有关质量法规、质量标准的规定及相关行业的标准。

3、乙方提供标准云平台的安全管理服务和安全技术服务，具备完备的安全防护体系和安全防护设备。

4、乙方提供的云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.9999%，云平台应按照等保三级标准建设并通过测评，云平台可按需 7 个自然日快速扩容。

5、乙方提供的云平台应具备资源动态调整机制，根据甲方信息系统运行情况进行资源的动态调整，如遇信息系统使用高峰期，经双方协商可短期内提供免费的云资源扩容服务，如需要长期使用扩容服务，以北京市级政务云基础服务目录价格为准双方协商费用，双方并签订补充合同。

6、乙方利用监控系统或人工对机房环境、硬件设备及应用系统的运行情况进行 7*24 小时的监控，及时发现安全隐患，并负责通知相关人员及时处理。

7、乙方应提供技术支持热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法，方式应包括邮件、电话、即时通讯工具等。邮件：bjs-govcloud@chinaunicom.cn ，电话：13241000380。

8、提供高效的系统监控，提供 7*24 小时现场和技术支持，在系统发生故障时 5 分钟内响应，在 30 分钟之内处理故障，可在 1 小时内到达运维现场提供技术支持。

9、在重大节假日及重保期间，根据甲方业务周期性特点，加大运维保障力度，安排人员值班值守，保证在业务高峰期内系统平稳运行。

10、乙方须具备故障快速定位和恢复能力，故障定位排除时限不超过 30 分钟，重要信息系统故障定位排除时限不超过 10 分钟。

第四条　项目小组及人员要求

甲乙双方应各指派一名代表作为本项目负责人，项目负责人职责范围包括：

1、跟踪项目执行：云服务使用培训，云服务各阶段验收，项目成果确认等管理工作。

2、项目检查和控制：检查云服务使用过程中各阶段工作质量和进度。协调各种资源，确保项目按计划进度实施。

3、项目沟通协调：负责协调解决组织接口及技术接口问题，沟通项目售前、售后情况，解决云服务使用过程中出现的相关问题。

4、甲方项目负责人及联系方式：刘印 18515372006；

5、乙方项目负责人及联系方式：李晴 18510005947；

第五条　执行期限

乙方为甲方提供为期 12 个月的政务云租用服务，自 2026 年 10 月 10 日起至 2027 年 10 月 9 日止。

第六条　项目验收

1、乙方以书面形式向甲方提交项目验收申请，甲方收到书面验收申请后组织验收工作。

2、在执行期满后 20 个工作日内对乙方项目执行情况进行验收。乙方应当在验收前向甲方提交验收材料，由甲方组织验收工作。验收不合格的，乙方应当在 15 日内进行调整，并重新提交甲方验收。

3、验收材料清单如下：

阶段	输出成果	备注
项目启动阶段	项目实施方案	
项目执行阶段	项目月报、项目专项服务报告等	
项目验收阶段	项目总结报告等	

第七条　项目费用及支付方式

1、本合同总金额共计人民币大写：肆佰壹拾万贰仟捌佰肆拾伍元肆角肆分（￥4,102,845.44），其中政务云租用云计算资源:2,194,393.44 元，政务云租用扩展资源：1,908,452.00 元。上述金额是乙方履行本协议的一切费用（含税）。除双方另有约定外，乙方不得要求甲方支付任何其他费用。

2、甲方分 2 次向乙方支付合同款项，以人民币结算。

（1）第一次支付：签订合同后，在执行期开始前，甲方向乙方支付合同款的60%，计人民币大写：贰佰肆拾陆万壹仟柒佰零柒元贰角陆分（￥2,461,707.26）。

（2）第二次支付：执行期满相关项目事宜办理完毕后，乙方交付所有工作成果及技术服务报告后，由甲方验收，经甲方验收通过后二十（20）个工作日内，进行剩余款项的支付。甲方向乙方支付本合同款的40%，计人民币大写：壹佰陆拾肆万壹仟壹佰叁拾捌元壹角捌分（￥1,641,138.18）。

（3）甲方每次按合同付款前，乙方应开具符合甲方要求的正式、等额、合法的发票，否则甲方有权拒绝付款且不承担违约责任，乙方不得因此暂停、中止履行义务。如乙方向甲方提供的发票不符合本合同约定或法律规定，因此给甲方造成的一切损失由乙方承担（包括但不限于损害赔偿、消除影响等）。

3、甲方付款单位为：北京市城市运行管理事务中心。

甲方付款单位税号：12110000MB1J66869N

因上级财政拨款导致甲方及其付款单位支付的迟延，不视为甲方及支付单位的违约。但甲方应当将延迟付款理由通知到乙方，且在支付限制解除后立即完成对乙方的付款。乙方不得因此延迟、拒绝、终止、暂停义务的履行。

4、乙方收款账户信息

开户名：中国联合网络通信有限公司北京市分公司；

开户行名称：中国工商银行北京长安支行；

乙方开户行账号：0200 0033 1921 0012 727；

第八条　甲方权利义务

1、甲方有权对乙方提供的各项技术支持和成果进行监督、检查和评价。

2、甲方应提出有关管理、技术需求和要求，协调乙方与信息系统供应商的关系，协调信息系统供应商配合调研、迁移、运维、安全和应急演练等过程的工作。

3、甲方需按照《北京市市级政务云管理办法》的要求申请、变更、退出云服务；在系统入云、上线、服务变更、退出等关键节点，甲方应提前提交《北京市市级政务云服务统一工单》相应部分内容至政务云管理单位进行备案作为工作依据。

4、甲方的信息系统在迁移、部署到乙方云平台之前，应开展必要的系统入云安全测试。

5、甲方负责本单位信息系统和相关基础软件的日常维护、管理、安全和应急保障。

6、甲方应确保部署在政务云平台的软件具有合法授权，不得擅自安装、使

用非法软件。

7、甲方如需对已上线信息系统进行维护升级、渗透测试、安全加固等操作，应提前告知乙方。

8、甲方有权要求乙方现场技术指导、处理故障及其他技术支持。

9、甲方有权要求乙方更换不符合本合同约定的技术支持人员，乙方应在5日内更换。

10、甲方其他的权利义务。

第九条　乙方权利义务

1、乙方须按照合同所约定的技术支持内容标准向甲方提供相关资源和技术支持。

2、乙方应协助甲方建立健全信息系统管理配套制度，包括：运维制度、应急预案、安全保障制度、运行监管办法等。

3、乙方负责云平台基础安全保障和运维工作。

4、乙方应负责本单位人员的安全培训、技术培训，确保工作人员符合岗位要求。

5、乙方需按照有关规定进行操作，确保各系统不被人为损坏。

6、乙方负责提供资源调度管理和维护，提供云主机状态监控，对甲方所购买使用的资源提供运维，未经甲方书面授权不得擅自修改信息系统数据或发布信息等。

7、乙方负责管理甲方申请的 IP 地址，为甲方提供 IP 地址分配和管理服务 。

8、信息系统正式上线后，乙方需定期向甲方提供政务云服务书面报告，以便甲方及时获取政务云资源或服务的使用情况。

9、甲方如需乙方提供重启服务器操作时，乙方有权要求甲方提供书面申请或其他可以证明甲方身份的信息，甲方提供了相应信息的，乙方应及时进行重启服务器等操作。除本款约定外，乙方原则上不接受甲方提出的其他可能对甲方服务器造成损坏的任何操作要求。

10、乙方应提供技术支持，以维护甲方系统的正常运行。

11、重大活动期间，乙方应配合甲方制定重保方案并提供云平台的现场值守等。

12、乙方应配合甲方制定信息系统应急预案，并配合开展信息系统应急演练工作，做好日常应急响应工作。

13、乙方接到甲方故障报告后，应及时做好相关信息的登记工作，并进行故障排查。乙方应定时向甲方反馈检查进度及结果，故障排除后，乙方应将结果及

时反馈甲方并做好书面报告和故障记录。

14、由于甲方指定的其他技术提供商提供的软件或产品的缺陷，造成的信息系统运行故障、安全漏洞、信息泄露等事故，乙方不承担相应责任，但需要按照甲方的要求协助和配合甲方进行整改。

15、当甲方入云信息系统出现严重影响政务云平台安全稳定运行的事件时，乙方有权暂时中断甲方的云服务并书面通知甲方，事件处理完毕后恢复。

16、乙方应保证为甲方提供具备本合同项下技术支持所需的相应资质和许可。乙方应保证技术人员在甲方工作过程中人员相对稳定。

17、乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有业务应用系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三方损失的，由乙方承担法律责任并负责赔偿相应损失。

18、乙方保证其履行合同义务不存在任何侵犯第三方著作权、商标权、专利权等合法权益的情形，否则乙方应赔偿因此给甲方造成的全部损失。

19、未经甲方事先书面同意，乙方不得转让本合同项下任何权利义务，不得擅自部分或全部转委托、分包项目的任何部分。

20、双方明确甲方与乙方技术人员不存在任何劳动、劳务、劳务派遣、委托等关系，亦不承担该人员的社会保险、福利待遇、工伤责任等。如乙方技术人员要求甲方承担任何与劳动、劳务、劳务派遣、委托关系等相关的法律责任、待遇等提起仲裁、诉讼等，乙方应承担甲方的损失。

21、乙方其他的权利义务。

第十条　安全责任边界

1、甲方安全责任

（1）　甲方承担本单位入云信息系统的基础软件、信息系统、数据等方面的安全责任。

（2）　甲方负责组织信息系统的应急演练，如有需要，甲方有权要求乙方配合应急演练。

2、乙方安全责任

（1）　乙方承担云平台层面（主要包括物理资源、计算资源、存储资源、网络资源）以及数据防篡改、防丢失的安全责任。

（2）　乙方在取得甲方书面许可后，开展云平台应急演练；乙方有义务配合甲方完成信息系统的应急演练。

（3）　乙方须按照《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14 号）的要求和有关网络安全标准，落实并通过所建设的云平台的第三方网络安全审查。

第十一条　知识产权归属

1、乙方保证向甲方提供的项目成果是其独立实施完成或取得相应授权，不存在任何侵犯第三方专利权、商标权、著作权等合法权益的情形。如因乙方提供的项目成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

2、双方在对外宣传（如在各自官网、市场营销活动）时，如有涉及对方的内容，应提前通知对方，在取得对方书面同意后方可发布信息 。

3、在本合同签订前已经存在的或履行过程中产生的其他与本合同无关的成果，包括但不限于设计方案、各种说明书、测试数据资料、计算机软件以及其他技术文档，知识产权归属原权利人所有。

4、本合同执行期间产生的包括但不限于相关电子文档（技术文档等）的知识产权归甲方所有。乙方应于本合同终止或甲方提出要求后 15 个工作日内，向甲方交付全部项目成果的完整原件、电子版本，乙方不得留存任何副本、备份或摘抄件。

第十二条　违约责任及合同解除

1、在运营期间，如发生附件 1 中所列 A 级事件 1 次，甲方有权以书面通知的方式解除本合同，并要求乙方赔偿甲方相应的经济损失。

2、在运营期间，如 1 年内发生附件 1 所列 B 级事件 3 次，甲方有权以书面通知的方式解除本合同，并要求乙方赔偿甲方相应的经济损失。

3、乙方履行合同过程中可能发生的违约行为及相应应承担的违约金详见附件 2、3 规定，甲方可从尾款中抵扣违约金。系同一事件导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，经甲乙双方协商，择其重者确定乙方支付违约金的办法。

4、在运营期间出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规定期限内未能履行甲方正当要求的，甲方有权与乙方解除本合同：

（1） 多次在云综合监管供应商已发出整改通知后未正确处置，出现问题并造成 B 级及以上事故；

（2） 重大活动期间所承诺的骨干人员和管理人员未到场；

（3） 连续 2 个月所承诺的运维人员人数未达到合同要求；

5、乙方逾期交付使用、逾期履行合同约定的义务或合同期满后经甲方验收不合格需进行整改的，每逾期一日，应承担合同价款千分之一的违约金；逾期超过 15 日，甲方有权以书面通知的方式解除本合同，并要求乙方赔偿甲方相应的经济损失。

6、甲方无正当理由逾期支付乙方合同款的，应承担合同价款万分之一的违

约金。

7、若因乙方的原因给甲方造成损失的，该损失包括但不限于甲方经济利益的减损、甲方为证实乙方之违约行为所支出的各项调查取证、公证费用，甲方为寻求救济而支付的诉讼费用、保全费、律师代理费、咨询费以及法院执行费用等。

第十三条　退出

1、执行期内，如乙方提出退出要求，需在执行期截止前至少 6 个月向甲方提出书面的退出申请，并获得甲方的许可并配合各方完成迁移和切换工作后方可退出，对于由此给甲方带来的经济损失，由乙方承担。

2、执行期内，如出现政务云管理单位责令乙方退出，在信息系统迁移和交接工作中，乙方应在甲方提出系统迁出需求后 10 天内配合甲方完成信息系统迁移的相关工作，包含梳理迁出系统的云资源、安全策略配置等。确保系统在新环境运行稳定后，关停原服务，并对原有系统数据进行安全擦除。前述费用及对甲方造成的损失由乙方承担。

3、执行期满后双方不再续签或者甲方提前解除合同的，乙方应无条件免费配合甲方完成迁移和切换工作，切换期为 1 个月。乙方承诺在切换期内配合完成迁移和切换工作。

第十四条　免责条款

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。

2、由于网络运营商的核心设备故障造成的网络中断、阻塞，从而影响到系统的正常访问或响应速率降低，属于不可控事件和不可抗力，甲方应对此表示认同。乙方应及时通知甲方并积极采取措施保障正常访问。

3、由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并在不可抗力发生之日起 15 天内提供相关政府部门或公证机关出具的证明文件。

4、由于不可抗力致使合同无法履行的，本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无须承担违约责任。不可抗力事件消除后，双方应就合同的履行及后续问题进行协商，按照该事件对合同履行的影响程度，决定继续履行合同或终止合同。

第十五条　保密条款

1、乙方因承接本合同约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为甲方的保密信息，乙方应按照法律法规及甲方关于保密工作的相关要求，对上述保密信息承担保密义务。未

经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。

2、乙方应对上述保密信息予以妥善保存，并保证仅将其用于与完成本合同项下约定项目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息，乙方应至少采取适用于对自己核心机密进行保护的同等保护措施和审慎程度进行保密。

3、乙方保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内，对乙方非从事该项目的人员一律严格保密。

4、乙方应保证在向其工作人员披露甲方的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为甲方的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密合同》。

5、任何时间内，一经甲方提出要求，乙方应按照甲方指示在收到甲方书面通知后 5 日内将含有保密信息的所有文件或其他资料归还甲方，且不得擅自复制留存。

6、非经甲方特别书面授权，甲方向乙方提供的任何保密信息并不包括授予乙方该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

7、乙方需要定期向政务云管理单位和云综合监管供应商提交云平台及入云系统相关信息，内容包括但不限于：云资源租用情况、系统迁移进展、已租用资源的使用绩效情况、安全监控分析、IP 管理、重大活动值守、工作建议等，此时如涉及甲方信息，不属于保密违约。

8、乙方承担上述保密义务的期限为长期，合同有效期间及合同解除或终止后，乙方均应履行上述保密义务，直至保密信息向社会公开。

9、承担上述保密义务的责任主体为乙方（含乙方工作人员）。如乙方或乙方工作人员违反了上述保密义务，给甲方造成损失的，乙方均应向甲方承担全部责任，并赔偿因此给甲方造成的全部损失。

10、乙方应对甲方提供的技术资料和数据等任何非公开信息负有保密义务，不得以任何形式、任何理由透露给第三方或擅自做本合同目的之外的使用。乙方的具体保密义务见附件《2026 年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统保密条款》。

11、乙方违反合同约定的保密条款，除立即停止违约行为外，还应当向甲方支付合同总额 20 %的违约金，甲方有权单方书面通知的形式解除合同，违约金不足以弥补甲方损失的，乙方应予以补足。

第十六条　争议的解决

1、本合同按中华人民共和国相关法律、法规进行解释。

2、因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列第（2）种方式解决：

（1） 提交北京仲裁委员会仲裁，仲裁裁决为终局裁决；

（2） 依法向甲方所在地有管辖权的人民法院起诉。

第十七条　合同内容变更

在本合同履行过程中，甲方提出项目需求变更，应与乙方协商一致并签署补充合同；在变更达成一致前，双方应继续履行其原约定义务。

第十八条　廉政承诺

1、合同双方承诺共同加强廉洁自律、反对商业贿赂。

2、甲方及其工作人员不得索要礼金、有价证券和贵重物品；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的超标准宴请和娱乐活动。

3、乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加超标准宴请及娱乐活动。

第十九条 技术支持

具体技术支持参数详见甲方2026年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统招标文件（项目编号：BGPC-G26194）中“项目需求”部分，及乙方的投标文件描述。

第二十条 其他

1、本合同自双方法定代表人或其委托代理人签名并加盖本单位公章或合同章后生效，至双方履行完毕本合同规定的全部义务时终止。

2、未尽事宜，经双方协商一致，签订书面补充合同，补充合同与本合同不一致的，以补充合同为准。

3、本合同一式陆份，甲、乙双方各执叁份，具有同等法律效力。本合同附件与本合同有同等法律效力。

4、双方确认本合同签署页载明的通讯地址为各方履行本合同及争议解决相关所有通知、文书的法定送达地址，任何书面通知按该地址寄出后三日内即视为有效送达。若任何一方变更送达地址，应当提前七日书面通知对方，未通知的，按原地址送达仍视为有效送达。

附件1：重大违约行为表

附件2：严重违约行为表

附件 3：一般违约行为表

附件 4：2026 年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统保密条款 本行以下无正文

（以下无正文）

（此页无正文）

甲方	名称(或姓名)	北京市城市运行管理事务中心			
	负责人	（签字）			
	委托代理人	（签字）			单位公章 2026年9月7日
	住　所 (通讯地址)	北京市西城区广安门内大街317号	邮政编码	100053	
乙方	名称(或姓名)	中国联合网络通信有限公司北京市分公司			
	负责人	（签字）			单位公章或合同专用章 2026年9月7日
	委托代理人	（签字）			
	住　所 (通讯地址)	北京市西城区骡马市大街9号	邮政编码	100025	

附件 1、 重大违约行为表

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（云服务商主责）	服务中断	云平台整体	因非不可抗力造成超过 30%以上信息系统中断、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	信息系统	在重大或特别重大保障期间，因云服务商的安全隐患原因造成的系统被恶意篡改事件。事件发生后云服务商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	等保三级或重要信息系统的核心业务数据	因非不可抗力造成的云平台超过 3个信息系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成信息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	云平台整体	因非不可抗力造成超过 10%至 30%信息系统中断、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	信息系统	因云服务商的安全隐患原因造成的系统被恶意篡改事件，事件发生后云服务商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、市级领导批示或关注的。	30 分钟以上		
	数据丢失	信息系统核心业务数据	因非不可抗力造成 1 个信息系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成信息系统被恶意篡改或敏感信息泄露事件。	——		

附件 2、 严重违约行为表

罚款金额=信息系统云服务费/执行月数*惩罚系数（惩罚系数参见《严重违约行为表》）

序号	问题描述	惩罚系数
1	所提供的云服务可用性低于 99.99%，或数据可用性低于 99.9999%，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，由于另一家云服务商服务中断，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	在云安全监管供应商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%
7	平均响应时间大于 15 分钟且小于 30 分钟，造成重大事故	200%
8	运维需求平均响应时间大于 30 分钟且小于 60 分钟，造成重大事故	200%
9	运维需求平均故障恢复时间大于 30 分钟且小于 60 分钟，造成重大影响	100%
10	运维需求平均故障恢复时间大于 60 分钟且小于 120 分钟，造成重大影响	200%
11	现场无人值守超过大于 1 小时且小于 2 小时，造成重大事故	100%
12	现场无人值守超过大于 2 小时且小于 4 小时，造成重大事故	200%

附件 3、 一般违约行为表

罚款金额=信息系统云服务费/执行月数*惩罚系数(惩罚系数参见《一般违约行为表》)

序号	问题描述	惩罚系数
1	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，出现问题但未造成重大损失的	50%
2	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，且在执行期内接到用户投诉此类情况 3 次以上的	20%
3	在运营期间，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	在运营期内，如乙方未能按照用户方的扩容需求，在 7 个自然日内完成云平台的资源扩容，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	在云安全监管供应商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%
8	运维需求平均响应时间大于 15 分钟且小于 30 分钟，出现问题但未造成重大影响	30%
9	运维需求平均响应时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	50%
10	运维需求平均故障恢复时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	30%
11	运维需求平均故障恢复时间大于 60 分钟且小于 120 分钟，出现问题但未造成重大影响	50%
12	现场无人值守超过大于 1 小时且小于 2 小时，出现问题但未造成重大影响	30%
13	现场无人值守超过大于 2 小时且小于 4 小时，出现问题但未造成重大影响	50%

附件 4、2026 年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统保密条款

鉴于，甲方：北京市城市运行管理事务中心、乙方：中国联合网络通信有限公司北京市分公司，签订了 2026 年北京市城市管理委员会政务云租用项目-城市运行监测、能源运行等系统的《项目合同》，在合同执行中乙方已经或将要知悉甲方的相关保密信息。为了保护上述合作中涉及的保密信息，明确双方的权利义务，甲、乙双方在平等自愿、协商一致的基础上达成以下条款：

一、安全要求

1. 乙方必须遵守甲方的各项规章制度，严格按照工作规范组织进行运维工作，制定切实可行的措施保障人员安全，设备安全，生产安全。

2. 乙方必须制定合理的措施对运维人员进行管理和思想教育，加强保密意识，安全生产意识。

二、保密信息范围

本条款所称的“保密信息”是指，乙方在合同履行过程中获得的下列信息，但不包括通过公众渠道可以获得的信息或经甲方书面同意允许向第三方透露的信息：

1. 工作秘密：一切与政府工作有关的信息资料或其他性质的资料，包括但不限于：政府业务数据、人员机构信息、财务资料等；

2. 技术秘密：指甲方的计算机信息系统、网络架构、信息安全体系结构、软件、数据库系统、系统数据、文档及技术指标等；

3. 其他保密信息：包括但不限于运维过程中获取的有关数据、流程、分析成果；甲方的内部管理资料、财务资料；甲方其他项目的信息及有关政府行政机关规划、调整等尚未公开的资料。

上述保密信息的表现形式不限，无论是书面的、口头的、图形的或其他任何形式的信息。

三、安全保密期限

本条款约定的保密责任期为长期，《项目合同》有效期间及合同解除或终止后，乙方均应履行上述保密义务，直至保密信息向社会公开，如在《项目合同》签订前乙方已实际接收或接触甲方保密信息的，则本条款的法律效力追溯至乙方实际接收或接触甲方保密信息之时，自该时起，乙方即应开始履行保密义务和责任。

四、保密义务人

本条款项下保密义务人为，乙方单位及乙方涉及保密信息的员工。

五、保密义务

乙方保证对所获悉的甲方保密信息按照下列规定进行保密，并在缺少相关保密条款约定时，应至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密：

1．仅将本条款项下保密信息使用于与运维工作有关的用途。

2．除直接参与运维工作的人员之外，不得将保密信息透露给其他无关人员

或任何第三方。

3．不能将甲方保密信息的全部或部分进行发布、传播、复制或仿造。

4．乙方均应告知并以适当的方式要求其直接参与运维工作的人员，按照本条款规定保守保密信息。如乙方工作人员违反本条款规定，泄露甲方保密信息的，乙方应承担违约责任。

5．乙方不能利用获悉信息为自己或其他方开发信息、技术和产品，或与甲方的产品进行竞争。

6．未经甲方书面许可并采取加密措施，乙方不得擅自将载有保密信息的任何文档、图纸、资料、磁盘、胶片等介质，带离甲方工作场所。

7．对于用户数据和项目结果数据的保管、访问，乙方无关人员不能访问；必需访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严格筛选。

8．对于甲方提供给乙方使用的任何资源，如网络、NOTES 等，乙方都只能将其用于工作，而不能用于其他目的，特别是从事侵害甲方利益的活动。

六、保密信息的交回

1.本项目涉及的运维相关工作终止后，乙方应按照甲方的要求对相关保密信息做相应处理，比如销毁或其他处理方式。

2.当甲方以书面形式要求交回保密信息时，乙方应当立即交回所有的书面或其他有形的保密信息以及所有描述和概括保密信息的文件。

3.未经甲方书面许可，乙方不得丢弃和自行处理保密信息。

七、争议的解决

因履行本条款而发生的或与《项目合同》有关的一切争议，双方应协商解决，协商不成的，双方均有权向甲方所在地有管辖权的人民法院提起诉讼。

八、其他

本条款未尽事宜，甲、乙双方另行签订补充条款，补充条款与本条款具有同等法律效力。