20260513000?

宣合同〔2026〕第27号

2026年文化和旅游局办公及业务系统信息基础支撑项目（第一包：云计算服务）

合同

甲方：北京市文化和旅游局宣传中心(北京市旅游运行监测中心)

乙方：北京金山云网络技术有限公司

甲方：北京市文化和旅游局宣传中心(北京市旅游运行监测中心)

法定代表人：康鹏遥

住所：北京市通州区留庄路 1 号院 1 号楼

电话：65158249

乙方：　北京金山云网络技术有限公司

法定代表人：　邹涛

住所：北京市海淀区西二旗中路 33 号院小米科技园

电话：010-62927777

甲、乙双方根据《中华人民共和国民法典》及相关法律法规的规定，在《北京市市级政务云管理办法》的基础上，经过友好协商，就乙方为甲方提供北京市政务云服务(下称"服务")事宜订立以下协议，以资共同遵守。

第一条 项目角色定义

1、使用单位：协议甲方，北京市文化和旅游局宣传中心(北京市旅游运行监测中心)（单位）。

2、云服务商：协议乙方，北京金山云网络技术有限公司（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 服务内容

1、本协议期限内，乙方向甲方提供如下云服务或云资源租用服务。甲方根据业务需要，与乙方协商确定选择云服务项目，

序号	服务子类	服务项	计价单位	单位	单价(元)	数量	服务期(月)	总价(元)	备注
1	云主机服务	Vcpu	元/个/月	个	14.02	1334	12	224,432.16	
2	云主机服务	内存	元/GB/月	GB	41.15	3408	12	1,682,870.40	
3	物理服务器租用	配置 1：双路每 CPU 核数≥32 核，主频 ≥2.0GHz，128G 内存，2 块 600GSAS 硬盘，2 个 HBA 卡，2 个万兆端口	元/台/月	台	300.00	5	12	18,000.00	
4	物理服务器增配	内存-32GB 内存	元/条/月	条	200.00	20	12	48,000.00	
5	物理服务器增配	硬盘配置 1-480GB SSD	元/块/月	块	122.00	25	12	36,600.00	
6	物理服务器增配	硬盘配置 3-4TBSATA	元/块/月	块	190.00	50	12	114,000.00	
7	普通性能存储	普通存储（单盘技术指标：单盘 IOPS 2000-5000）	元/GB/月	GB	0.28	104874	12	352,376.64	
8	高性能存储	高性能存储（单盘技术指标：单盘 IOPS 10000-25000）	元/GB/月	GB	0.64	63480	12	487,526.40	
9	静态存储	提供大容量、高可靠的数据存储服务，具备 PB 级线性扩展能力	元/GB/月	GB	0.07275	20000	12	17,460.00	
10	本地云主机备份	本地备份服务	元/GB/月	GB	0.88	20000	12	211,200.00	
11	互联网链路	提供多线运营商接入服务，保证稳定可靠	元/Mb/月	MB	49.55	360	12	214,056.00	
12	互联网 IP 地址	提供互联网地址租用，并且提供网站域名备案服务	元/个/月	个	76.05	35	12	31,941.00	
13	主机负载均衡	提供数个主机应用集群负载均衡服务	元/个/月	个	10.00	7	12	840.00	
14	远程接入服务	每个账号结合身份验证通过 VPN 远程接入堡垒机维护	元/个/月	个	356.00	23	12	98,256.00	
15	WAF 防护	为每个 ip 提供 web 应用防火墙服务	元/个/月	个	98.00	35	12	41,160.00	
16	国产商用操作系统套餐	国产商用操作系统套餐服务	元/套/月	套	300.00	58	12	208,800.00	
17	国产数据库管理系统套餐	国产数据库管理系统套餐服务	元/套/月	套	4,300.00	4	12	206,400.00	

18	商用操作系统套餐	Windows Server 套餐：Windows Server 租用、安装及维护。	元/套/月	套	120.00	34	12	48,960.00	
19	云端 APT 防护服务	对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁	元/套/月	套	1,200.00	2	12	28,800.00	
20	主机杀毒服务	通过云平台集成的杀毒软件，对云主机进行定期的病毒查杀，杀毒软件采用集中控制，云主机端无需安装代理软件，病毒库升级采取控制端统一下发的方式，对网络性能无影响。	元/vm/月	vm	12.00	119	12	17,136.00	
21	主机防护服务	提供符合等保三级要求的主机权限管理及安全防护。可对服务器系统安全涉及的控制点（如身份鉴别、敏感标记、强制访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防护和资源控制等）形成立体防护，解决操作系统层面面临的恶意代码执行、越权访问、数据泄露、破坏数据机密性、完整性等各种攻击行为，以保障数据及业务系统的保密性、完整性、可用性、可靠性。	元/台/月	台	1,800.00	35	12	756,000.00	
22	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。	元/次	次	1,500.00	119	12	178,500.00	
23	网页防篡改服务	提供网页防篡改服务。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。	元/次	次	1,600.00	120	12	192,000.00	
24	重点保障-安全专家服务	主要提供与安全相关的人工服务，安全隐患分析、安全培训、应急处置服务、木马病毒分析、日志隐患分析等服务。分析报告、人工协助解决隐患、解决方案等	元/人天	人天	2,000.00	20	12	40,000.00	

25	安全风险评估	对现有系统提供非破坏性的远程安全监测与安全风险评估，将外部访问、系统维护、资源使用等信息汇总。提供系统安全分析，包括可疑访问、恶意访问分析等安全隐患的预警性分析。	元/套/月	套	1,650.00	1	12	19,800.00	
26	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。	元/次	次	1,500.00	119	12	178,500.00	
27	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。	元/次	次	1,000.00	476	12	476,000.00	
28	数据库审计服务	实现数据库操作审计，记录每次数据库操作并整理报告。	元/套/月	套	1,200.00	10	12	144,000.00	
29	数据库许可服务	Sql Server 数据库许可服务。	元/套/月	套	6,000.00	1	12	72,000.00	
30	基于国密算法的远程安全接入	支持在终端与平台之间建立 SSL VPN 安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的 HTTPS 安全通道（3 个账号）。	元/个/月	个	500.00	3	12	18,000.00	
31	密钥管理服务	提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理。	元/套/月	套	9,000.00	1	12	108,000.00	
32	数据加密服务	提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护；支持文件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率 100Mbps。	元/套/月	套	5,500.00	1	12	66,000.00	

33	签名验签服务	提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持 SM2 签名速度不低于 700 次/秒。	元/套/月	套	2,000.00	1	12	24,000.00	
34	虚拟密码机 (VSM) 服务	基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例 4C8G。	元/VSM/月	VSM	8,000.00	1	12	96,000.00	
35	密码 API 接口服务	把密码调用接口进行业务级封装形成统一密码服务 API 和 SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。	元/套/月	套	13,000.00	1	12	156,000.00	
36	国密 SSL 证书	国密 SM2 服务器证书 SSL V3 型，支持通配，需要 IP 验证可以是 80/443 端口，域名验证可以选择邮箱或 DNS；根据浏览器识别地址栏显示绿标；证书主题显示：单位名称和所在省市；配套购买 RSA 算法的 SSL 证书。	元/张/月	张	1,800.00	1	12	21,600.00	
37	国密浏览器服务	提供符合国密要求的国产浏览器服务功能安装在用户 PC 端，通过安全浏览器访问业务系统（3 个/月）。	元/个/月	个	120.00	3	12	4,320.00	
38	智能密码钥匙（usbkey）	PC 终端密码支撑服务，PC 端用户身份认证。业务系统每个用户配发一个。含数字证书（3 个/月）。	元/个/月	个	40.00	3	12	1,440.00	
39	集中式存储租用	提供集中式存储用于支持 Oracle RAC 5000G/月。	元/GB/月	GB	0.50	5000	12	30,000.00	
	合计(元)							6,670,974.60	

第三条 服务水平

1、乙方应为甲方提供本协议约定的全部服务，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、乙方应配合甲方搭建信息系统上云的测试环境，免费测试期由甲乙双方协商确定。

3、乙方为甲方提供的服务质量应符合国家、北京市有关质量法规、质量标准的规定及相关行业的标准。

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，云平台可按需在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，并签订补充协议。

6、乙方应提供技术服务热线(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：ksc_kingstack_service@kingsoft.com，电话：010-62927777。

7、乙方在服务期内，提供7*24小时的现场和技术支持服务，对故障15分钟内响应；如故障无法远程排除2小时内派员到达云中心机房。

8、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，各方项目负责人职责范围包括：

1、制定项目计划：牵头制定项目计划。

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

3、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。

4、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。

5、甲方项目负责人及联系方式：刘栋 010-55526031 。

6、乙方项目负责人及联系方式：郑钧军 13911101261 。

第五条 服务期限

乙方为甲方提供为期 12 月的政务云资源租用服务，自 2026 年 5 月 14 日起，至 2027 年 5 月 13 日止。

第六条 服务验收

1、甲方依据本协议，在服务期满前 20 个工作日内对乙方服务情况进行最终验收。乙方应当在验收前向甲方提交验收材料。验收合格的，甲方在验收合格单上签字，并对乙方服务质量进行评价；验收不合格的，乙方应当在 5 日内进行返工或调整，并重新提交甲方验收。

2、验收材料清单如下：*（下表内容可根据实际情况调整）*

阶段	输出成果	备注
系统运行阶段	政务云运维服务方案、巡检计划	
	云服务运维月报（含云平台巡检报告）	
	安全巡检月报	
	故障处置记录	按实际
	政务云运维月报、半年报（如有）	按需求
	安全漏洞扫描报告（如有）	按需求
	渗透测试报告（如有）	按需求
	其他（云平台重大事件通知、异常预警、重保期间值守记录等）	
阶段性验收阶段	政务云服务阶段性总结报告（半年报和年报）	

第七条 服务费用及支付方式

1、本协议总金额共计人民币小写（含税）：6,670,974.60 元，大写：陆佰陆拾柒万零玖佰柒拾肆元陆角整。

2、自本协议签署之日起，且政府采购财政资金拨付到账后 15 个工作日内，甲方向乙方支付人民币：4,002,584.76 元，大写：肆佰万贰仟伍佰捌拾肆元柒角陆分 ；乙方需向甲方提供等额的法定正规发票。

3、乙方通过甲方中期检查后 15 个工作日内，甲方向乙方支付人民币：1099187.52 元，大写：壹佰零玖万玖仟壹佰捌拾柒元伍角贰分 ；乙方需向甲方提供等额的法定正规发票。

4、乙方提供本协议项下的全部服务内容并经甲方终验合格之日起 15 个工作日内，甲方向乙方支付人民币：1569202.32 元，大写：壹佰伍拾陆万玖仟贰佰零贰元叁角贰分。乙方需向甲方提供等额的法定正规发票。

5、乙方收款银行账户信息如下：

户名：北京金山云网络技术有限公司

开户行：民生银行上地支行

账号：0110012830003054

乙方保证上述信息真实、准确，乙方的上述账户信息发生变化的，应至少于甲方付款5个工作日前书面通知甲方，否则由此导致的错付、无法支付等所有法律后果均由乙方自行承担。

第八条 甲方权利义务

1、甲方有权对乙方提供的各项服务进行监督、检查和评价。

2、甲方及信息系统服务商应提出有关管理、技术需求和要求。

3、甲方应协调乙方与信息系统服务商的关系，协调信息系统服务商配合调研、迁移、运维、安全和应急演练等过程的工作。

4、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。甲方应按本协议约定使用乙方提供的云资源，做到资源专用，协议未约定或未提交《北京市市级政务云服务统一工单》至政务云管理单位备案的信息系统不得部署入云。

5、甲方及信息系统服务商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、甲方及信息系统服务商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、甲方及信息系统服务商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、甲方及信息系统服务商有权要求乙方现场技术指导、处理故障及其他服务。

9、甲方其他的权利义务：_____无_____。

第九条 乙方权利义务

1、乙方须按照协议所约定的服务内容标准向甲方提供相关资源和服务。

2、乙方应在甲方的信息系统迁移、部署到乙方云平台之前，对其开展必要的系统入云安全测试。

3、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。

4、乙方负责云平台日常维护、管理、安全和应急保障。

5、乙方应负责本单位人员的网络安全培训、技术培训，确保工作人员符合岗位要求。

6、乙方需按照有关规定进行操作，确保各系统不被人为损坏。

7、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服务，经授权对甲方信息系统的应用和数据库提供可用性监控服务，未经授权不得访问甲方的信息系统和数据库，不得擅自修改信息系统数据或发布信息等。

8、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 。

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

10、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。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。

11、乙方应提供及时的技术支持服务，以维护甲方系统的正常运行。

12、重大活动期间，乙方应配合甲方制定重点保障方案并提供云平台的现场值守等服务。

13、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。

14、乙方接到甲方或甲方信息系统服务商故障报告后，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。

15、由于甲方或甲方信息系统服务商指定的其他技术服务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，但需要配合甲方或甲方信息系统服务商进行整改。

16、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通知甲方，事件处理完毕后恢复服务。

17、未经甲方同意，乙方不得将合同义务委托第三方完成。

18、乙方其他的权利义务：_____无

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《中央网络安全和信息化领导小组办公室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[2014]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服务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。如因乙方提供的服务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，在取得对方同意后方可发布信息 。

3、在本协议签订前已经存在的或履行过程中产生的其他与本协议无关的成果，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、本协议执行期间产生的相关电子文档（技术文档等）的知识产权归甲乙

双方所有，各自均有权单独使用该文档。

第十二条 违约责任及协议解除

1、在运营期间，如发生附件 1 中所列 A 级事件 1 次，或违反保密义务的，乙方应按本合同金额的 5%承担违约金，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,无条件配合甲方完成迁云，承担迁云费用。

2、在运营期间，如发生附件 1 所列 B 级事件 3 次，乙方应按本合同金额的 5%承担违约金，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、无条件配合甲方完成迁云，承担迁云费用。

3、乙方提供服务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*（附件中的罚款即指乙方出现相关违约行为/问题时应支付的违约金）*，从第二期款或尾款中抵扣。系同一事件或原因导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，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满足甲方正当要求，影响甲方正常使用的，甲方有权与乙方解除协议,乙方应无条件配合甲方完成迁云，承担迁云费用，并与以上支付违约金的规定一并适用：

（1）三次及以上在云监管服务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 60 日所承诺的运维服务人员人数未达到协议要求；

（4）另一家云服务商提出“双活”需求，不给予配合*（可选）*。

5、因乙方违约，甲方为维护自身合法权益而支出的包括但不限于调查取证

费用、公证费、评估费、鉴定费、保全费、保全担保费或保全担保保险费、律师代理费、咨询费、差旅费等均由乙方承担。

第十三条 退出

1、服务期内，如乙方提出退出要求，需在服务期截止前至少 6 个月向甲方书面提出退出申请，并获得甲方的许可后方可退出，对于由此给甲方带来的经济损失，由乙方承担。

2、服务期内，如出现政务云管理单位责令乙方退出，相关补偿费用甲乙双方另行协商；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。

3、服务期满后双方不再续签或者甲方提前解除协议的，乙方应无条件免费配合甲方及第三方完成迁移和切换工作，切换期为 60 日。

第十四条 免责条款

1、本协议中不可抗力指地震、台风、火灾、水灾、战争、罢工、公共卫生事件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，参照不可抗力事件处理。

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

4、由于不可抗力致使协议无法履行的，本协议在不可抗力影响范围及其持续期间内将中止履行，本协议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，双方应就协议的履行及后续问题进行协商，按照该事件对协议履行的影响程度，决定继续履行协议或终止协议。

第十五条 保密条款

1、乙方因承接本协议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《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施条例》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协议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《保密协议》。

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或立即销毁，且不得擅自复制留存。

6、非经甲方特别授权，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监管服务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协议有效期间及协议终止后。

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、未经过双方事先书面同意，双方不得使用对方商标（包括但不限于文字、图形等）、logo、品牌标识等，双方不得就本协议的合作关系、未来可能或实际进行的合作及项目进行对外公开、宣传和发表公开言论（包括但不限于网站、新闻、报纸、微博、微信、公告、宣传单、海报等）。如果就特定事宜需要进行对外公开、宣传和发表公开言论，需要事先获得对方书面确认对外公开、宣传和发表公开言论的内容。本条款有效期追溯至甲乙双方初次建立合作之日。

第十六条 争议的解决

1、本协议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 协议内容变更

在本协议履行过程中，甲方提出服务需求变更，应与乙方协商一致并签署补充协议；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 其他

1、本协议自双方法定代表人或其委托代理人签名并加盖本单位协议专用章或单位公章后生效，至双方履行完毕本协议规定的全部义务时终止。

2、未尽事宜，经双方协商一致，签订书面补充协议，补充协议与本协议不一致的，以补充协议为准。

3、本协议一式 六 份，甲、乙双方各执 三 份，具有同等法律效力。

4、协议附件为本协议不可分割的组成部分，与协议正文具有同等法律效力。

（以下无正文）

附件：

附件 1 重大违约行为

附件 2 严重违约行为

附件 3 一般违约行为

甲方：北京市文化和旅游局宣传中心

（北京市旅游运行监测中心）

（盖章）

法定代表人或

授权代表：

签订日期：2026年5月14日

乙方：北京金山云网络技术有限公司

盖章）

法定代表人或

授权代表：

签订日期：2026 年 5 月 14 日

开户行：民生银行上地支行

开户名：北京金山云网络技术有限公司

账号：0110012830003054

附件 1：重大违约行为

表：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。	30 分钟以上	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。	30 分钟以上		
	数据丢失	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 1 个信息系统丢失超过 1 个月以上（包含一个月）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 1 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	30 分钟以上	B 级	3 次及以上
	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。	30 分钟以上		
	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

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

表：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	在云安全监管服务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%
13	连续 3 个月未能按时按要求提交项目月度服务报告，无法提供云服务工作证明。	300%

附件 **3**：一般违约行为

罚款金额=信息系统云服务费/服务月数*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%，且在服务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	在云安全监管服务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%