合同编号：HAPYS2600111ECN00

濮阳市行政审批和政务信息管理局
关于濮阳市市级政务云服务项目
第三标段合同书

项目名称：濮阳市行政审批和政务信息管理局

关于濮阳市市级政务云服务项目第三标段

甲方：濮阳市行政审批和政务信息管理局

乙方：中国电信集团有限公司濮阳分公司

签订地：河南濮阳

签订日期：2026年 2月 4日

2026年1月16日，濮阳市行政审批和政务信息管理局以公开招标形式对濮阳市行政审批和政务信息管理局关于濮阳市市级政务云服务项目第三标段进行了采购。经评标委员会评定，中国电信集团有限公司濮阳分公司为该项目中标供应商。现于中标通知书发出之日起三十日内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经濮阳市行政审批和政务信息管理局（以下简称：甲方）和中国电信集团有限公司濮阳分公司（以下简称：乙方）协商一致，约定以下合同条款，以兹共同遵守、全面履行。

1.1 合同组成部分

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标通知书；

1.1.3 投标文件（含澄清或者说明文件）；

1.1.4 招标文件（含澄清或者修改文件）；

1.1.5 濮阳市政务云服务项目实施方案；

1.1.6 其他相关采购文件。

1.2 标的

1.2.1 标的名称：政务云云计算服务；

1.2.2 标的数量：1 批；

1.2.3 标的质量：合格。

1.3 价款

乙方按照濮阳市实际资源需求量开展本次建设工作，保障当前紧急业务云资源需求。乙方按照濮阳市政务云服务项目实施方案和服务目录提供政务云服务。如根据项目需求要新增服务目录项，需由甲乙双方沟通，服务内容及价格协商一致并经过评审后，双方签订补充协议。

计费方式：遵循“先用后付、先审后付、据实结算”的原则，服务期每满一年后，乙方将本年度服务费金额及计算方式书面报甲方审核，服务资源实际使用量以甲方审核同意的各市级部门实际使用的云资源单元内容和数量为准。按照实际使用的服务内容、数量，服务目录的单价进行计费，据实结算。按照乙方中标价格执行即服务目录价格的 89.5%折扣执行。

分项价格：

本次采购包含基础设施资源服务：包括网络资源服务、计算资源服务、存储资源服务。基于云计算的高弹性、高可靠性、高冗余的特点，采用可行的云计算模式，向各用户提供统一的 IT 资源服务，包

括不限于云主机、云存储、云备份等服务。

信息安全技术服务：包括安全防护服务、用户安全服务、安全接入服务、安全管理服务、安全扫描服务、网站防护服务，密码资源池等相关服务。

一朵云一道墙运营服务：包括“一道墙”安全运营支撑平台、流量监测系统（1Gbps）、流量监测系统（7Gbps）、安全检测系统、域名监测系统、网络威胁防御系统、“一朵云”综合管理平台。

以下列出的“单价”均指含税价。具体如下：

类型	名称	说明	规格	单元最高限价（元/月）
计算	云主机（普通）	两核	2GB	79
			4GB	95
			8GB	128
		四核	4GB	157
			8GB	190
			16GB	255
		八核	8GB	314
			16GB	380
			32GB	510
			64GB	771
		十六核	16GB	628
			32GB	759
			64GB	1020
			128GB	1543
			256GB	2587
		三十二核	32GB	1257
			64GB	1518
			128GB	2041
			256GB	3085
			512GB	5174
		核（vCPU）	1 核	31
		内存（G）	1GB	8
	高性能物理机	CPU≥2 路 6 核，内存≥64GB，本地硬盘>=600GB		1274

		CPU≥2 路 8 核，内存≥256GB，本地硬盘>=600GB		1415
		CPU≥2 路 10 核，内存≥320GB，本地硬盘>=600GB		1555
		CPU≥2 路 10 核，内存≥256GB，本地硬盘≥6TB		1682
		CPU≥2 路 10 核，内存≥256GB，本地硬盘≥6TB，SSD 硬盘≥1.92TB		1729
		CPU≥2 路 10 核，内存≥256GB，本地硬盘≥33.2TB，SSD 硬盘≥1.92TB		2361
		CPU≥2 路 14 核，内存≥320GB，本地硬盘>=600GB		1836
		CPU≥4 路 10 核，内存≥256GB，本地硬盘≥600GB		2558
		CPU≥4 路 14 核，内存≥320GB，本地硬盘≥600GB		3120
		CPU≥8 路 10 核，内存≥512GB，本地硬盘>=600GB		4442
		CPU≥8 路 14 核，内存≥512GB，本地硬盘≥600GB		5687
		CPU≥8 路 16 核，内存≥512GB，本地硬盘≥600GB		6249
	国产化高性能物理机	2 路 32 核 CPU，256GB 内存，2 块 480GB SATA SSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		2464
		2 路 48 核 CPU，256GB 内存，2 块 480GB SATA SSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		2904
		2 路 64 核 CPU，256GB 内存，2 块 480GB SATA SSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		3344
	高性能物理机可选配件	32GB 内存	1 块	76
		1TB SAS 硬盘	1 块	37
		1TB SATA 硬盘	1 块	19
		1TB SATA SSD 硬盘	1 块	69
		1TB NVME SSD 硬盘	1 块	197
		HBA 卡	1 块	138
		万兆网卡（含模块）	1 块	97
	AI 加速卡	不低于 16GB 显存，峰值算力不低于 96TOPS FP16	1 块	834
		不低于 24GB 显存，峰值算力不低于 96TOPS FP16	1 块	1557

		不低于 48GB 显存，峰值算力不低于 128TOPS FP16	1 块	3058
	数据库 一体机	数据库计算资源（实例）	1 核 8GB	1073
			2 核 16GB	2052
			4 核 32GB	4103
			6 核 48GB	6156
			8 核 64GB	8208
			10 核 80GB	10259
		数据库存储	1GB	0.56
备份	本地数据备份服务		1TB	164
	异地数据备份服务		1TB	179
	冷数据备份服务		1TB	48
存储	块存储（普通）	IOPS≥3000	1TB	167
	块存储（高效）	IOPS≥10000	1TB	333
	对象存储（低频）	IOPS≥500	1TB	83
	对象存储（普通）	IOPS≥1000	1TB	117
	文件存储（普通）	IOPS≥1000	1TB	117
	文件存储（高效）	IOPS≥10000	1TB	333
网络	负载均衡	最大连接数 10000	1 实例	52
基础软件	操作系统软件		1 套	110
	数据库软件		1 套	922
	Web 中间件软件		1 套	400
机柜托管	机柜空间	机柜空间（1U）	1U	230
	机柜托管	按照 42U 标准服务器机柜，宽度 600mm，深度 1200mm。含供电、制冷等标准配套	个	3300
容器服务	容器服务	容器服务，不包含计算资源	1 节点	150
云数据库服务	关系型数据库	两核	4GB	462
		四核	8GB	1016
		八核	16GB	2034
		十六核	32GB	4437

		十六核	64GB	5566
		三十二核	64GB	8873
		三十二核	128GB	12059
		存储空间	GB	0.31
	缓存数据库		4GB	309
			8GB	619
			16GB	1238
			32GB	2475
			64GB	4950
			128GB	9899
		存储空间	GB	0.31
	分布式数据库	四核	16GB	1089
		四核	32GB	1213
		八核	32GB	1955
		八核	64GB	2426
		十六核	64GB	3911
		十六核	128GB	4852
		三十二核	128GB	9703
		三十二核	256GB	13467
		存储空间	GB	0.31
云中间件服务	分布式中间件服务、微服务	两核	8GB	473
		四核	16GB	918
		八核	32GB	1655
		十六核	64GB	3002
人工智能服务	人工智能开发平台	提供机器学习模型训练、部署、服务等功能	1 实例	6000
大数据计算基础资源	离线计算	提供批量结构化数据的存储和计算	1CU（1 核+4GB）	300
			存储容量 1GB	0.31
	流式计算	提供流式计算引擎	1CU（1 核+4GB）	360
	实时数仓	提供对海量数据进行即时的多维分析透视和业务探索，快速构建数据仓库。	1CU（1 核+4GB）	249
			存储容量 1GB	0.31
	全文检索	提供数据分析、搜索等场景服务	数据节点 4 核 16G	1140
			数据节点 8 核 32G	2200
			数据节点 16 核 32G	3190
			数据节点 16 核 64G	4356
			主节点 4 核 16G（默认 3 节点）	3432

			主节点 8 核 32G（默认 3 节点）	5896
			主节点 16 核 32G（默认 3 节点）	9570
			主节点 16 核 64G（默认 3 节点）	13112
			Node4 核 16G	1140
			Node8 核 32G	2200
			Node16 核 32G	3190
			Node16 核 64G	4356
			存储 SSD（1GB）	0.31
			存储高效云盘（1GB）	0.16
安全服务	入侵检测服务	为云上系统提供南北向的网络层入侵检测服务，支持漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、暴力破解等的检测和防护，防护带宽≥50Mbps。	1IP	288
	WEB 应用防火墙服务	为云上 Web 应用系统提供应用层安全防护服务，支持 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护，http/https 协议防护带宽≥50Mbps。	1IP	288
	漏洞扫描服务	漏洞扫描系统，对云主机系统进行漏洞扫描，输出检测报告，提供修复建议。	1IP	10
	网页防篡改服务	实时监测和保护站点内容安全，防止非法篡改网页，保护站点公众形象。	1IP	168
	堡垒机服务	提供运维安全管理与审计系统，支持主机管理、权限控制、运维审计等功能。	1IP	24
	主机杀毒服务	提供主机杀毒功能，对云主机进行全面的病毒扫描、检测、清除和防护。	1 客户端	18
	虚拟防火墙	提供网络虚拟化防火墙及入侵防御安全能力	VM	288
	虚拟 VPN 安全接入	提供移动办公安全接入，包括接入用户身份认证、传输	VM	300

		数据加密、权限划分和接入审计，每 100 个 VPN 并发组件		
	日志审计服务	提供日志审计系统，对租户云主机、应用、网络设备等操作日志审计，支持日志采集、日志存储、日志检索、日志分析、可视化统计等。	1 日志源	48
	数据库审计服务	提供数据库审计系统，对数据库的操作行为审计，对各类数据库访问行为进行解析、分析记录。	1 实例	898
	服务器安全防护	提供虚拟化主机安全轻代理防护能力，有效防御服务器端的黑客入侵和恶意代码，并融合微隔离、资产清点、风险管理、补丁管理、基线检查、webshell 检测、攻击溯源等一体化服务器安全管理功能。	1IP	240
	东西向安全检测服务	支持给服务器按需配置流量采集转发策略，支持查看服务器业务流速和转发流速，并可查看生效策略，同时记录操作历史，并外发至流量采集器	1IP	500
密码服务	密钥管理服务	为租户提供密钥生成、存储、更新、备份、恢复及归档等密钥全生命周期管理。 性能规格： 并发请求数≥100 次/秒， 密钥存储量≥10000 个。	1 套	1588
	加解密服务	提供标准 API 接口，为业务系统提供应用级数据加解密、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护。性能规格： 并发请求数≥128 次/秒， SM1 计算速率≥15Mbps， SM2 加密≥2300 次/秒， SM2 解密≥1000 次/秒， SM4 计算速率≥150Mbps。	1 系统	1448

	签名验签服务	基于数字签名、验证签名技术，为业务系统提供应用级数字签名、验证签名等服务。性能规格： 并发请求数≥128 次/秒， SM1 计算速率≥15Mbps， SM2 加密≥2300 次/秒， SM2 解密≥1000 次/秒， SM4 计算速率≥150Mbps。	1 系统	1648
	SSLVPN 接入服务	面向运维侧为租户提供基于国密数字证书认证方式的安全接入，提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道（只提供账户服务，不包含数字证书 USBkey）	1 账户	2.2
	IPSECVPN 服务	为租户提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道。性能规格：吞吐率≥500Mbps，最 大并发隧道数≥1000 个。	1 套	886
	时间戳服务	提供时间戳签发、时间戳响应、时间戳解析、时间戳和有效性等多种安全功能。用于实现数据时间认证与签名 需求奠定坚实基础。性能规格：时间戳并发量≥100 个/秒， 时间戳签发≥80 次/秒， 时间戳验证≥150 次/秒。	1 系统	550
	安全认证服务	为业务系统提供基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务。 性能规格：最大用户数≥500，加密吞吐量≥500Mbps。	1 系统	1876
	协同签名服务	用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥	1 套	1826

		生成、密钥签名、密钥解密、密钥协同功能。性能规格：身份认证≥1000 次/秒，并发速率≥1000，数字签名≥2000 次/秒，并发数≥100。		
	数据库加密服务	提供数据库加密服务，实现对数据库关键字段或全库的数据进行加密保存，满足结构化数据的存储机密性及完整性要求。性能规格：SM4 的加密性能≥70Mbps，数据库操作性能损耗≤20%，加密性能≥5000QPS。	1 实例	1888
	文件加密服务	提供非结构化文件加密服务，保障用户数据安全对非结构化文件提供加密服务，保障用户数据安全。性能规格：文件读写操作性能损耗≤20%，文件加密速率≥400Mbps。	1 系统	1888
	电子签章服务	支持 SM 系列国产密码算法。采用标准的电子印章和电子签章编码格式以及验证规范。具有人员管理、部门管理、数据库备份、电子印章管理、电子印章生成和下载、日志审计和设备自检等功能。	1 系统	1688
	数字认证服务	具有高可靠性的安全机制及完善的管理及配置策略，可以提供自动化地密钥和证书管理服务，支持多操作系统。系统对整个证书的生命周期进行管理，主要功能包括初始化、系统管理、证书模板管理、RA 管理、CA 证书服务、CRL 管理、证书发布、日志审计和接口服务等。	1 系统	4530
政 务	常态化安全服	提供安全服务团队，对政务	个	1500 元/人/

云配套服务	务	云提供安全事件研判、事件评估、代码安全检测、APP评估、渗透测试、流量分析溯源、重保服务、安全加固以及应急处置等常态化安全服务，并定期按要求提供相应的安全服务报告。		天
一道墙服务	“一道墙”安全运营支撑平台	“一道墙”安全运营支撑平台包括安全数据集、资产管理、威胁情报、安全检测、安全监测、安全预警、能力服务、应急响应、协同处置等功能模块，安全数据集作为一体化安全运营支撑平台的底层数据安全底座，统一管理采集设备、数据解析规则和策略，实时监控多方面状态。其涵盖日志采集与处理、流量采集与处理、安全数据处理、安全数据存储、安全数据库管理等多个方面。在资产管理上，采用“主动扫描 + 被动获取”方式识别网内终端和服务器，实现全面管理和安全态势分析。威胁情报方面，内置情报库，实现精准威胁发现和多源情报汇聚及上下级共享，为安全运营提供全面支持。安全检测具备完善脆弱性监测功能，实现全生命周期管理。安全监测通过分析数据检测异常行为，为安全运维提供可视化页面和全面安全态势呈现。安全预警依托平台汇聚多元数据，通报涉事单位协调处置。能力服务打破安全能力孤岛，实现自动化运维和安全事件处置。应急响应通过应急预案和威胁情报实现全方位支撑和有效处置。协同处置采集处理资源数据，	套	121002

		协同决策处置，增强协作能力。地市平台与省级平台联通对接，实现能力上下贯通、情报数据共享和多部门联合工作机制，共同保障安全事件及时处理和漏洞整改，为构建安全、高效的网络安全生态体系奠定坚实基础。		
	流量监测系统	流量监测系统可以针对网络流量 APT 攻击的高级威胁检测和分析系统，可掌握全政务网络的流量来侦测并响应 APT 攻击与未知威胁。流量监测系统部署在客户网络中负责接入流量的监控。从流量和文件两个维度，并结合海量威胁情报，来精准发现未知威胁的恶意行为，同时根据不同的威胁种类和攻击手法做特定的研判和聚合，在大量减少告警数量的同时给出精准的威胁判断。	套	33565
	安全检测系统	安全检测系统可以针对政务网络资产进行常态化脆弱性检测，提供对系统漏洞、WEB 漏洞、网站漏洞、数据库等脆弱性进行评估。通过脆弱性评估能力能够全面、精准地检测信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等。在信息系统受到危害之前为管理员提供专业、有效的漏洞分析和修补建议，防患于未然。	套	12626
	域名监测系统	域名监测系统可以在政务外网部署域名监测系统，在域名解析统一管理的基础上，提高了自动化、安全性、智能化等方面的能力，提供	套	10522

		域名安全防护，通过域名威胁情报共享、域名智能解析、溯源审计、网络及终端可视、故障快速定位等核心网络功能，实现对企业网络稳定性、安全的有效保障。		
	网络威胁防御系统	网络威胁防御系统通过网络威胁防御系统集成病毒查杀引擎，实现在网络边界，针对 Windows 和 Linux 下的挖矿、勒索、灰色软件、木马、蠕虫等病毒进行精准查杀；持续优化高性能流扫描引擎、网络威胁检测引擎，有效阻止挖矿攻击及其他网络事件入侵、漏洞利用攻击、 暴力破解、APT 攻击、C&C 外联等恶意行为，能够针对 1DAY、NDAY 漏洞进行快速响应，有效保护用户网络内部的数据资产安全；集成 Web 信誉查杀引擎，有效阻止网站挂马攻击、跨站脚本攻击和网络钓鱼等，保护 Web 服务器的安全。	套	21149
	攻防演练服务	网络攻防与安全渗透演练：10 系统及以下攻防演练。（依托专业化技术平台，在保障业务系统安全性的前提下，组织开展实战攻防对抗。按照演练约定，攻击方在靶标范围内组织攻击，防守方组织安全防护，进行实战攻防对抗。严格落实“全程监控、全程审计、全程可视、全程管理”等技术管控措施，确保演练攻击程度既接近实战，又“点到为止”避免影响系统正常运行。	次	111400/次

一朵云服务	“一朵云”安全运营服务	“一朵云”综合管理平台需要具备多云纳管能力，统一纳管政务云各类云的计算资源、存储资源、网络资源，并以图、表方式展示各云平台资源使用情况，包括总CPU、内存、存储等的资源总量、已分配容量、未分配容量、资源使用率，能够自定义设置政务云服务目录，支持按年、月、日等计费方式，可通过平台选择资源使用量进行费用计算，可批量对各种场景的云资源进行新建、变更、释放等申请；可统一根据各资源池的资源使用情况进行资源分配；可统一对政务云使用进行调度，并以清单形式展示云资源调度情况；可统一对云资源情况进行实时监测，以可视化形式展示云资源使用率、运行状况、剩余情况等数据；统一将政务云与省“一朵云”综合管理平台对接上报。	套	21044
等保测评服务	等保测评服务	根据《中华人民共和国网络安全法》及《信息安全等级保护管理办法》，按照安全等级要求对信息系统进行测评/复测	1 系统/次	31000/次
政务通三网短信	政务通三网短信	政务通平台所需三网短信服务	条	0.05 元/条
维护服务	软硬件平台维护	平台软硬件的运行维护、相关培训等服务	根据实际需求订购	根据实际需求订购

网站云监测服务	网站云监测服务	通过云端防护技术，并实时防护网站可用性监测、网站挂马监测、网站篡改监测、网站黑链/暗链监测、网站敏感词监测、仿冒/钓鱼网站监测、网站 DDOS 攻击监测、漏洞情报分析、态势感知分析、态势感知呈现。	200M/租户	1500

注：清单中未涉及到的项目，如发生额外费用，由双方另行协商解决，按照实际发生费用签订补充协议另结算。

1.4 付款方式和发票开具方式

1.4.1 付款方式:遵循“先用后付、先审后付、据实结算”的原则，服务器每满一年后，乙方将本年度使用费金额及计算方式书面报甲方审核，服务资源实际使用量以甲方审核同意的各市级部门实际使用的云资源单元内容和数量为准。按照实际使用的服务内容、数量，服务目录的单价进行计费，据实结算。经专家或第三方机构验收后进行支付。按照乙方中标价格执行即服务目录价格的 89.5%折扣执行。

甲方每年服务期满后 30 天之内支付款项。

1.4.2 发票开具方式：按照相关规定提供正规增值税普通发票。

1.5 履行期限、地点和方式

1.5.1 履行期限：本次合同期限为一年，根据服务质量与资金落实情况，次年度可以续签，总体合同最多三年。

（1）次年度续签需满足以下条件：①年度服务可用性达标（≥99.99%）；②无 3 级及以上信息安全责任事故；③年度验收合格；

（2）甲方有权根据年度服务质量评估结果（以验收报告为准）决定是否续签，无需向乙方支付任何补偿。

1.5.2 履行地点：采购人指定地点。

1.5.3 履行方式：合同签订后，二十日内按合同要求完成交付；

1.6 违约责任

1.6.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，那么甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务价格的 1%计算，最高限额为本合同总价的 3%；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

（1）服务可用性未达到 99.99% 的，每低于 0.01 个百分点，扣除当月服务费的 1%；单个应用服务中断时间超 262.8 分钟的，超出部分每分钟扣除服务费 500 元，最高限额为本合同总价的 3%；

（2）发生数据泄露、丢失事件的，乙方需承担甲方全部实际损失（含直接损失、合规处罚、数据恢复费用等），同时扣除 20 万元服务费；若为 3 级及以上安全责任事故，甲方有权单方解除合同，乙方已履行的部分甲方应据实结算，未履行的部分不再履行；

（3）资源交付响应时间超 3 个工作日的，每逾期 1 日扣除该资源对应服务费的 5%，逾期超 7 日的，甲方有权取消该资源订单并要求乙方赔偿损失

1.6.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 1%计算，最高限额为本合同总价的 3%；迟延付款的

违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

1.6.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，对方当事人可以书面通知违约方解除本合同；

1.6.4 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

1.7 合同争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；拒绝和解、调解或者和解、调解不成的，可以选择下列第 1.7.2 种方式解决：

1.7.1 将争议提交 / 仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.7.2 向乙方住所地管辖的人民法院起诉。

1.8 合同生效

本合同自双方当事人盖章并签字时生效，如使用电子章的，自各方盖章之日起生效，合同内容以乙方加盖电子章的版本为准。

合同编号：HAPYS2600111ECN00

甲方：濮阳市行政审批和政务信息管理局

法定代表人（或授权代表）签字：

日期：2026年2月4日

乙方：中国电信集团有限公司濮阳分公司

法定代表人（或授权代表）签字：

日期：2026年2月4日

第二部分 合同一般条款

2.1 定义

本合同中的下列词语应按以下内容进行解释：

2.1.1“甲方”系指与中标供应商签署合同的采购人；

2.1.2“乙方”系指根据合同约定提供服务的中标供应商；

2.2 技术规范

服务所应遵守的技术规范应与采购文件规定的技术规范和技术规范附件（如果有的话）及其技术规范偏差表（如果被甲方接受的话）相一致；如果采购文件中没有技术规范的相应说明，那么应以国家有关部门最新颁布的相应标准和规范为准。

2.3 知识产权

乙方应保证其提供的服务不受任何第三方提出的侵犯其著作权、商标权、专利权等知识产权方面的起诉； 如果任何第三方提出侵权

指控，那么乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿；

2.4 履约检查和问题反馈

2.4.1 甲方有权在其认为必要时，对乙方是否能够按照合同约定提供服务进行履约检查，以确保乙方所提供的服务能够依约满足甲方之项目需求，乙方应予积极配合；

2.4.2 合同履行期间，甲方有权将履行过程中出现的问题反馈给乙方，双方当事人应以书面形式约定需要完善和改进的内容。

2.4.3 乙方无条件提供“一朵云”管理平台和统一安全运维监管接口，并接受甲方指定的监管平台监管。

2.5 结算方式和付款条件

结算时，按照实际使用的服务内容、数量，服务目录的单价进行计费，据实结算。按照乙方中标价格执行即服务目录价格的 89.5%折扣执行。

甲方每年服务期满后 30 天之内支付款项。

详见合同专用条款。

2.6 技术资料和保密义务

除非依照法律规定或者对方当事人的书面同意，任何一方均应保证不向任何第三方提供或披露有关合同的或者履行合同过程中知悉的对方当事人任何未公开的信息和资料，包括但不限于技术情报、技

术资料、商业秘密和商业信息等，并采取一切合理和必要措施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。

（1）保密范围包括甲方政务数据、业务流程、技术参数、合同条款、资源使用情况等所有未公开信息；

（2）乙方的保密义务期限为合同签订之日起至合同终止后 5 年；

（3）乙方需建立专门保密制度，对接触甲方信息的人员进行专项培训并签订保密协议，甲方有权定期核查。

2.7 质量保证

2.7.1 乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2.7.2 乙方应保证履行合同的人员数量（驻场人员主备模式：原政务云不少于 2 人，新政务云不少于 4 人，总数不少于 6 人）和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

（1）驻场人员需具备 3 年以上政务云运维经验，持有云计算相关认证，人员名单及资质证明需经甲方审核确认；

（2）驻场人员更换需提前 15 日书面告知甲方，经甲方同意后方可更换，更换后人员资质不得低于原人员标准，每月更换人数不得超过总驻场人数的 30%；

（3）乙方需确保驻场人员全时在岗（工作日 9:00-18:00，节假

日安排值班），脱岗累计超 3 日的，按每日 5000 元扣除服务费。

2.7.3 服务质量评价应满足附件（政务云服务水平协议）。

2.8 延迟履行

在合同履行过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长履行的具体时间。

2.9 合同变更

2.9.1 双方当事人协商一致，可以签订书面补充合同的形式变更合同，但不得违背采购文件确定的事项，且如果系追加与合同标的相同的服务的，那么所有补充合同的采购金额不得超过原合同价的 10%；

2.9.2 合同继续履行将损害国家利益和社会公共利益或遇上级重大政策出台、调整等因素，确无法继续履行的，双方当事人应当以书面形式变更合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

2.10 合同转让和分包

合同的权利义务依法不得转让，但乙方可以依法采取分包方式履行合同，接受分包的人应当具备相应的资格条件，并不得再次分包，且乙方应就分包项目向甲方负责，并与分包供应商就分包项目向甲方承担连带责任。

2.11 不可抗力

2.11.1 如果任何一方遭遇法律规定的不可抗力或上级重大政策出台、调整等因素，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间；

2.11.2 因不可抗力或上级重大政策出台、调整等因素，致使不能实现合同目的的，当事人可以解除合同；

2.11.3 因不可抗力或上级重大政策出台、调整等因素，致使合同有变更必要的，双方当事人应在合同专用条款约定时间内以书面形式变更合同；

2.11.4 受不可抗力影响的一方在不可抗力发生后，应在合同专用条款约定时间内以书面形式通知对方当事人，并在合同专用条款约定时间内，将有关部门出具的证明文件送达对方当事人。

2.12 税费

与合同有关的一切税费，均按照中华人民共和国法律的相关规定缴纳。

2.13 乙方破产

如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同且不给予乙方任何补偿和赔偿，但合同的终止不损害或不影响甲方已经采取或将要采取的任何要求乙方支付违约金、赔偿损失等的行动或补救措施的权利。

2.14 合同中止、终止

2.14.1 双方当事人不得擅自中止或者终止合同；

2.14.2 合同继续履行将损害国家利益和社会公共利益的，或因上级重大政策出台、调整导致合同确需中止或终止，双方当事人应当中止或者终止合同。

出现以下情形之一的，甲方有权书面通知乙方单方解除合同，无需承担违约责任：

（1）乙方发生 3 级及以上信息安全责任事故，或数据泄露事件累计 2 次及以上；

（2）服务可用性连续 2 个月低于 99.9%，或年度累计未达标次数超 3 次；

（3）乙方未按约定提供驻场人员，或驻场人员资质不达标且逾期未整改；

（4）乙方擅自转让合同义务，或无正当理由拒绝配合甲方变更需求、履约检查。

2.15 检验和验收

2.15.1 乙方负责提供计算资源、存储资源等相关服务，每月向甲方及政务云使用单位提供政务云运行维护报告、资源使用情况优化建议或动态调整意见；

2.15.2 合同期满或者履行完毕后，甲方有权组织（包括依法邀请国家认可的质量检测机构参加）对乙方履约的验收，即：按照合同约定的标准，组织对乙方履约情况的验收，并出具验收书；向社会公

众提供的公共服务项目，验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告；

2.15.3 检验和验收标准、程序等具体内容以及前述验收书的效力详见合同专用条款。

2.16 通知和送达

2.16.1 任何一方因履行合同而以合同第一部分尾部所列明的送达方式发出的所有通知、文件、材料，均视为已向对方当事人送达；任何一方变更上述送达方式或者地址的，应于7个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达方式或者地址仍视为有效。

2.16.2 以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

2.17 特别约定

详见合同专用条款约定

2.18 合同份数

合同份数按合同专用条款规定，每份均具有同等法律效力。

第三部分 合同专用条款

本部分是对前两部分的补充和修改，如果前两部分和本部分的约定不一致，应以本部分的约定为准。本部分的条款号应与前两部分的条款号保持对应；与前两部分无对应关系的内容可另行编制条款号。

条款号	约定内容
2.5	付款条件和要求：遵循"先用后付、先审后付、据实结算"的原则，服务期每满一年后，乙方将本年度服务费金额及计算方式书面报甲方审核，服务资源实际使用量以甲方审核同意的各市级部门实际使用的云资源单元内容和数量为准。 结算时，按照实际使用的服务内容、数量，服务目录的单价进行计费，据实结算。按照乙方中标价格执行即服务目录价格的89.5%折扣执行。 甲方每年服务期满后30天之内支付款项。
2.11	一方当事人因不可抗力或上级重大政策出台、调整等不能按照约定履行本合同的，根据不可抗力的影响，可部分或全部免除责任，但应当及时告知对方，并自不可抗力结束之日起15日内向对方当事人提供证明。

2.18	不收取履约保证金。
2.19	根据《河南省加强数字政府建设实施方案（2023-2025 年）》（豫政（2023）17 号）、《关于加强全省数字政府一体化统筹建设的意见》（豫办发电（2023）16 号）、《河南省政务云整合工作方案》（豫数政办（2023）7 号）等相关要求，乙方应配合甲方在规定时间内完成对满足迁移条件的现有政务云存量政务信息系统的整合迁移和云资源的统一纳管。
2.20	本合同一式捌份，其中甲方肆份，乙方肆份，具同等法律效力。

附件：政务云服务水平协议

政务云服务水平协议

一、服务可用性

（一）指标定义

（1）计划内停机时间

乙方提前通知且经甲方认定的，为系统正常升级、更新、维护导致的服务停机。

（2）服务中断时间

乙方提供的机房、网络、安全、虚拟机、物理机、存储、运维等方面出现的问题引起应用系统失效时间，经甲方认定由非乙方原因引起的系统失效不包含在内。

（3）正常服务运行时间

当年总运行时间（按 365 天计算）减去服务中断时间。

（4）服务可用性

正常服务运行时间除以该年总运行时间，即：

服务可用性＝(365x24x60x60 秒一单个应用失效时间之和（秒）)/(365x24x60x60 秒）（闰年按照 366 天计算）。

（二）指标要求及测量方法

(1）指标要求

政务云平台的服务能力须保证各个应用系统可用性不低于 99.95%。即全年单个政务应用失效时间之和不超过 365x24X60x0.0005=262.8 分钟。连续 3 个月或累计 6 个月未达标时，甲方有权终止合同，并要求乙方赔偿业务损失。

(2）测量方法

序号	指标名称	测量方法
1	正常服务运行时间	向甲方或第三方提供测量结果查看接口，并确认检查结果
2	服务中断时间	向甲方或第三方提供测量结果查看接口，并确认检查结果

(3）补偿或赔偿

乙方的单个应用服务可用性指标未达到要求的 99.95%，服务中断时间超过该时间要求的则每分钟扣除服务费 500 元人民币。连续 3 个月未达标或全年累计中断超过 30 小时的，甲方有权单方终止合同并要求乙方支付年度服务费 10%的违约金；乙方需在服务中断后 2 小时内提供临时应急方案，并在 24 小时内恢复正常服务，否则每延迟 1 小时额外扣罚 1 万元。

一、信息安全责任事故考核

（一）指标定义

信息安全责任事故是指由乙方提供的机房、网络、安全、虚拟机、物理机、存储、运维等方面出现问题引起的信息安全责任事故。经甲方认定由非乙方引起的信息安全责任事故不包含在内。

（二）指标要求及赔偿办法

根据安全责任事故对政务应用系统造成后果的严重程度，安全责任事故划分为 5 个等级。其中 1 级危害程度最高，5 级危害程度最低。3 级和 3 级以上的信息安全责任事故称为重大安全责任事故。

表 2 安全责任事故指标测量方法表

分级	描述	扣款金额	备注
1	对电子政务云平台所承载的应用系统造成灾难性的危害，并对事发单位的利益造成灾难性的损失。	赔偿相应损失并处以 20 万元扣款	追究相应法律责任
2	对电子政务云平台所承载的应用系统有极其严重的影响或破坏，并对事发单位的利益造成严重危害。	赔偿相应损失并处以 10 万元扣款	追究相应法律责任
3	对电子政务云平台所承载的应用系统造成较为严重的影响或破坏，并对事发单位的利益产生一定危害。	赔偿相应损失并处以 5 万元扣款	
4	对电子政务云平台所承载的应用系统及事发单位的利益有一定的影响和破坏。	赔偿相应损失并处以 2 万元扣款	
5	对电子政务云平台所承载的应用系统及事发单位的利益基本不影响或损害极小。	处以 1 万元以下扣款	

三、系统保密考核

因乙方原因，导致发生数据外泄等系统保密事件，乙方应承担由此给甲方造成的实际损失，甲方保留追究乙方责任的权利。

四、资源交付服务响应时间

（一）指标定义

资源交付服务响应时间是指乙方接到甲方书面政务云服务资源需求后到资源交付的时间。

（二）指标要求

表 3 资源交付服务响应时间指标要求表

序号	指标名称	服务应达到的指标	考核周期	其他要求
1	资源交付服务响应时间	不超过 3 个工作日	年	

（三）指标测量方法

表 4 资源交付服务响应时间指标测量方法表

序号	指标名称	测量方法	测量接口
1	资源交付服务响应时间	交付时间-提交时间	

（四）补偿或赔偿

乙方的资源交付服务响应时间指标未达到要求，乙方应在 30 天内整改，并赔偿该资源延期时间对应的服务费。超过 3 个工作日的，每延迟 1 日扣减对应服务费 0.1%（最高不超过该资源价值的 5%）；延迟超过 5 日的，甲方有权自行采购第三方资源，费用由乙方全额承担。

五、应急响应

(一)指标要求及赔偿办法

乙方应根据事件的级别，按表 5 要求及时对事件进行响应。

表 5 指标要求及赔偿办法表

时间类型	事故级别	时长	赔偿及补偿办法
事件响应时间	特别重大	5 分钟	超过 5 分钟，则每分钟扣除服务费 500 元人民币
	重大事件	10 分钟	超过 10 分钟，则每超 5 分钟扣除服务费 500 元人民币
	一级事件	30 分钟	超过 30 分钟，则每 10 分钟扣除服务费 500 元人民币

(二)指标定义

(1)事件响应时间指乙方接到事件通知开始至维护人员到场及时上报的时间，事件响应时间确定需要甲方认可。

(2)事故级别划分：

1)特别重大：故障造成系统失效或崩溃，应用系统无法正常启动运行、网络故障、丢失数据等，且没有临时替代解决方案；系统硬件故障、系统崩溃(死机和自动重启)且不能再启动、磁盘信息丢失、系统或应用服务无法启动、网络链接失效、文件损毁等。

2)重大事件：故障造成系统发生中断或系统死机但重启后正常；应用部分不稳定；系统运行正常，但不能进行操作(控制台无响应).

3)一般事件：故障对系统业务无明显影响，仅造成系统报错、非关键应用无法启动、使用不便、操作不畅等。

(三)应急演练

乙方应制定详细的《应急演练方案》，内容包括但不限于政务云平台的网络、存储、备份等，并按方案进行应急演练，服务期内应不少于 2 次。若缺失《应急演练方案》，则扣款人民币 5 万元；若全年应急演练次数少于 2 次，每少一次，扣款人民币 5 万元。

(四)事件响应报告

乙方在处理完事件后，应将事件相关情况报告甲方。事件响应报告至少应包括以下内容:

(1) 事件的类别；(2)事件的级别；(3)事件发现时间:(4)事件的通报时间；(5)事故解决时间；(6)受影响的系统；(7)影响残留(未能解决的问题)

六、培训

乙方应向甲方提交《培训计划》并得到认可。乙方按计划组织培训，培训内容包括服务流程和服务资源使用方法等。若方未按《培训计划》进行，则甲方有权扣款人民币 5 万元；若全年总培训次数少于 2 次，则按每次人民币 5 万元执行扣款。因甲方原因未达到上述要求，乙方不承担任何责任。