

北京市药品监督管理局

信息化系统运行维护—安全和基础运维服 务-云服务器及网络管理维护服务合同书

2026 年

签约地点：北京



甲 方：北京市药品监督管理局

地 址：北京市通州区留庄路 6 号院 2 号楼

邮政编码：101117

联 系 人：王永清

电 话：010-55526959

传 真：

乙 方：北京银信长远科技股份有限公司

地 址：北京市朝阳区安定路 35 号安华发展大厦 8 层

邮政编码：100029

联 系 人：朱冲冲

电 话：010-82629666

传 真：010-82621118

甲乙双方依据《中华人民共和国民法典》及其他相关法律法规的规定，在平等自愿的基础上，同意按照下面的条款和条件，签署本合同。

一、定义

1、“合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

2、“合同价款”系指根据合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价款。

3、“资料”指乙方在合同项下，向甲方提供的所有印刷或打印的文件，通过任何方式（包括声像或文本）和任何媒介向甲方提供的各种指令性和信息性的帮助，但不包括口头指导。

4、“知识产权”指本合同涉及的任何及所有的著作权、商标权、专利权和
其它智力成果的和专有的权利和利益。

5、“甲方技术部门”是指代表甲方行使或履行合同中约定甲方技术部分权
利义务的甲方内部职能部门。

6、除有特别说明外，“天”、“日”均指日历日。

二、合同的组成

以下文件是本协议不可分割的组成部分

- 1) 本合同
- 2) 招标文件
- 3) 投标文件文件
- 4) 保密协议
- 5) 成交通知书
- 6) 本合同附件一、附件二

三、合同金额和服务期限

1、乙方为甲方提供维护服务，本合同总价款（含税）为：人民币大写：陆拾贰万肆仟肆佰捌拾元整，小写：¥624480.00 元。

2、服务期限：自合同生效且乙方提供有效服务之日起 12 个月。

四、维护服务内容及要求

具体服务内容及要求详见：招投标文件及本合同附件。

五、服务质量考核

甲方每季度将对乙方的驻场运维服务质量进行客观评估，以甲方用户满意度为核心考核依据，填写《运维服务评分表》（详见附件一），评分结果作为乙方服务质量的最终评定标准。

考核评分标准：以《运维服务评分表》满分 5 分为基准，乙方在任意一次季度考核中，平均分未达到 3 分（含 3 分）的，乙方需选择以下任一方式承担违约责任：

（1） 免费延长甲方相应运维服务期限一个月；

（2） 以本次考核对应周期，按照合同总金额千分之五（5%）的标准支付违约金。

若乙方累计 3 次（含3次）季度考核平均分未达到 3 分（含3分），甲方有权单方解除本合同，并要求乙方承担总金额10%的违约金。由此给甲方造成损失的，如违约金不足以弥补甲方损失的，不足部分甲方有权向乙方追偿。

本合同约定的运维服务全部结束后，甲方将对各季度《运维服务评分表》结果进行汇总、归纳，综合评定乙方的总体服务质量，评定结果作为合同尾款支付的参考依据之一。

六、合同价款的支付

1、本合同中甲乙双方之间所发生的一切费用以人民币进行结算。

2、本合同中甲方应向乙方支付的总价款为（含税）：

3、支付方式：

3.1 本项目合同款项为（含税）：大写：陆拾贰万肆仟肆佰捌拾元整，小写：¥624480.00，甲方应当在合同签订后40个工作日内向乙方支付本合同 40% 的服务费款项，即人民币24.9792万元；在合同约定的服务期过半且乙方前期服务通过甲方中期验收后，甲方向乙方支付本合同 30% 的服务费款项，即人民币18.7344万元。在本合同约定的服务期届满并通过甲方验收后40个工作日内，扣除违约金（如有）、赔偿金（如有）后甲方向乙方支付合同剩余款项。

3.2 乙方应于甲方支付相应费用前，先行向甲方出具符合甲方要求的等额增值税普通发票。否则，甲方有权拒绝付款，且不因此承担违约责任。

甲方应付至以下乙方指定的银行账户：

开户名称：北京银信长远科技股份有限公司

开户银行：兴业银行北京海淀支行

账 号：321230100100025629

七、甲方的权利义务

1. 甲方有权提出服务工作要求及标准，有权对乙方的服务工作进行指导、监督；
2. 甲方有权对乙方服务质量的评审和验收。甲方指派项目联系人（王永清）全权代表甲方进行项目各种协调和实施管理工作，并对乙方提交的过程文档进行考核和确认；
3. 乙方人员如发生违反合作约定或未做好履行合同准备等导致或即将导致伤害甲方利益、影响服务质量等行为，甲方有权随时提出整改，要求乙方撤换服务人员，并有权追究乙方的违约责任；
4. 甲方负责协助本项目的外部关系的协调；
5. 甲方负责提供合同约定的履行本合同所必备的与工作有关的项目资料。

八、乙方的权利义务

1. 乙方应具备履行本合同约定服务的专业资质和服务团队，完成能够胜任本合同约定项目的运维服务。
2. 乙方派驻人员需具备履行本合同义务的专业资质和服务经验，并将派驻人员名单和派驻人员专业资质证书作为本合同附件；乙方应接受甲方对服务工作的领导、监督、检查，管理派驻服务人员。
3. 乙方应严格按照本合同要求，提供规定范围内各项服务，每月定期总结并向甲方报告运维工作，严格按照合同约定保证服务的质量和服务及时性。
4. 乙方运维服务应如实进行工作记录，根据甲方的服务要求，按时保质完成工作，运维各项工作应提交规范、完整、真实、准确的数据和文档，并定期向甲方报告；

5. 乙方服务人员应统一着装，持证上岗，严格遵守甲方的规章制度和安保、安全等要求。

6. 乙方使用甲方提供的设施和物品属于甲方的财产，在服务工作完成或中止时，应将其设施和剩余的物品库存清单提交给甲方，并及时移交此类设施和物品；

7. 项目实施过程中，乙方如因正当理由需要调整项目技术人员的，应当提前5日通知甲方，获得甲方书面同意后方可进行。

8. 乙方及乙方服务人员严禁利用维保设备及接入的电路从事危害国家安全、泄露国家机密、侵害用户合法权益的违法犯罪活动，不得查阅、制作、复制甲方的工作信息及内部资料，不得传播妨碍社会治安的任何信息。

9. 乙方向甲方提供的专业驻场服务（节假日期间，按需驻场），负责设备维护工作。甲方特殊工作任务及需要临时进行服务保障的，乙方应增派人员全天候提供保障，确保系统正常运行维护。

10. 乙方对履行合同过程中的安全负全责。乙方及乙方工作人员履行合同过程中，造成自身或他人人身伤害或财产损失的，由乙方承担全部法律责任。因此导致甲方承担责任的，甲方有权予以追偿。甲方有权中止或终止履行合同，产生的经济损失由乙方承担。

九、违约责任

1、除本合同另有约定外，维护期内如果因乙方原因造成未能按合同约定提供服务（含提供服务达不到合同要求或逾期提供服务等），甲方可按次向乙方扣减本合同总金额千分之五的违约金，并有权要求乙方整改。整改仍不符合甲方要求或合同约定的，乙方应向甲方承担合同总价款30%的违约金，造成甲方损失的，另行承担赔偿责任，且甲方有权解除本合同。

2、除本合同另有约定外，当发生以下情形之一时，甲方有权解除合同并有权要求乙方支付合同总价款30%的违约金；违约金不足以弥补甲方全部损失的，乙方应当予以补足：

(1) 乙方或其工作人员违反本合同约定的保密义务；

(2) 乙方提交的服务内容侵犯（或可能侵犯）其他任何第三方知识产权或其他合法权益；

(3) 乙方部分转让或全部转让其应履行的合同义务；

(4) 乙方所提供服务存在严重瑕疵或重大缺陷；

(5) 乙方资质、提供服务人员等情况的真实性存在重大瑕疵或相应的资质失效；

3、因乙方服务问题造成事故，使得甲方设备遭受损失或造成网络安全重大事故等影响甲方正常使用和不良影响的，乙方应向甲方承担不少于合同金额 30% 的违约金，并赔偿相应损失，甲方有权解除合同。

4、乙方违约造成甲方的费用的增加和损失，甲方有权从剩余合同款项中直接扣除。如待支付的合同剩余款项不足以弥补甲方上述费用和损失，乙方应向甲方支付不足部分款项。

十、知识产权及保密

1、乙方保证，其根据本合同提供的产品及服务没有任何权利瑕疵，没有侵犯任何第三方权利，甲方在使用该产品或服务的任何一部分时，免受第三方提出的侵犯其知识产权的起诉。如果任何人对甲方使用该产品或服务主张权利，由乙方负责处理一切纠纷及相关事宜。由此给甲方造成的损失，由乙方承担，其承担范围包括但不限于：赔偿费、律师费、仲裁费和与仲裁相关的费用。

2、甲方尊重乙方软件产品的著作权，不在甲方以外的第三方做非法复制和扩散。

3、合作期间双方同意保守在缔结和履行合同过程中获知的对方保密信息，除一方履行合同义务的必要或法律、法规规定应披露的之外，不得以任何方式向第三人披露和不正当使用，否则，应当赔偿因泄露保密信息给对方造成的损失。

4、本合同无论何种原因终止，本条款继续有效。

十一、不可抗力

1、由于发生不能预见、不能避免并不能克服的不可抗力情形，致使直接影响本合同的履行或不能按照本合同项下之约定履行时，遇有不可抗力的一方应当立即书面通知对方，并在发生不可抗力之日起30日内，提供不可抗力详情及合同不能履行或部分不能履行，或延期履行的书面证明，该项证明文件应当由不可抗力发生地的公证机关出具。

2、根据不可抗力对本合同的影响程度，双方应当协商是否解除本合同或部分免除履行本合同的责任，或延期履行本合同。

十二、合同争议的解决

因本合同引起与本合同有关的一切争端应首先通过双方友好协商解决。如果协商不能解决，任何一方均应当向甲方所在地人民法院提起诉讼，且诉讼期间，除正在进行审理的部分外，本合同其它部分应继续履行。

十三、合同的转让及更改

1、未经甲乙双方同意，任何一方不得将本合同规定的权利和义务转让给第三方或委托第三方代理。维护服务期内，乙方如发生债权债务变动或关联公司战略重组需经甲方同意并认可方案。

2、对本合同作任何更改或补充，必须经甲乙双方代表协商签字并加盖公章或合同章后方可生效。

十四、合同的生效及其他

1、本合同自双方授权代理人签字并加盖公章或合同章之日起生效，合同一式肆份，甲方贰份，乙方贰份。

2、本合同未尽事宜，按中华人民共和国有关法律、法规办理。

甲方(盖章):



法定代表人或授权代表人

(签字):

林静

乙方(盖章):



法定代表人或授权代表人

(签字):



签字日期:

2026.04.27

签字日期:

2026.04.27

附件一：运维服务评分表

合同名称:					
服务商:		考核年度:			
考核描述	很不满意	不太满意	基本满意	满意	很满意
考核分值	1	2	3	4	5
定期巡检服务质量					
同样问题或故障是否重复出现					
排障服务及时性					
服务质量					
工程师的技术水平					
考核结论:					
甲方考核部门公章:			乙方经办人签名:		
年 月 日			乙方盖章:		
			年		
			月 日		

附件二：维护服务内容

云服务器管理、运维管理及运维过程监控；网络设备维保以及网络管理、策略配置优化及 IP 地址（IPV4, IPV6）管理。其中维保的网络设备清单如下：

序号	设备名称	设备型号	单位	数量
1	服务器	华为 H5885 V2	台	1
2	网络设备	华为 AR2220	台	3
3	网络设备	华为 S12708	台	3
4	网络设备	华为 S5700	台	3
5	网络设备	华为 SVN2260	台	1
6	网络设备	绿盟 RSAS NX3	台	2
7	网络设备	网康 5000	台	1
8	网络设备	深信服 ADC5000	台	1
9	网络设备	深信服 ADC8000	台	2
10	网络设备	天融信 NGFW4000	台	1
11	网络设备	天融信 NGFW4000-UF	台	1
12	网络设备	天融信 NGFWARES-V	台	1
13	网络设备	天融信 Topaduit TF-5248-bj	台	1
14	网络设备	网御 2800AV-c	台	1
15	网络设备	网御 3800	台	1
16	网络设备	网御 N820P	台	2
17	网络设备	IBM KVM	台	1
18	服务器	华为 SMC2.0 视讯业务管理系统	台	1
19	服务器	华为 MCU 多点控制单元	台	1

（二）项目服务期

自合同生效且供应商提供有效服务之日起 12 个月。

（三）项目服务地点

北京市药品监督管理局。

二、技术服务要求

（一）服务器统一管理

对云服务器实现统一管理，确保的稳定安全运行，包括但不限于以下内容：

1、建立服务器管理规范：制定详细的服务器管理规定和管理台账，明确云服务器的需求审核、开通、使用、操作和维护流程。确保所有操作符合规范，杜绝因不规范操作导致的问题。

2、服务器监控与日志分析：实时监测服务器的性能指标和运行状态。同时，收集和分析服务器的日志信息，及时发现异常和潜在问题。

3、建立应急响应机制：针对云服务器故障或安全事件，建立应急响应机制。明确应急流程、责任人员和恢复措施，确保在紧急情况下能够快速响应和恢复。

（二）远程登录账号管理

对云主机远程登录账号进行统一管理，包括但不限于以下内容：

1、账号权限管理：根据运维人员的职责和工作需求，为每个运维人员分配适当的远程登录账号及权限。避免出现权限过高或过低的情况，确保账号权限的合理性和安全性。

2、账号生命周期管理：建立账号生命周期管理制度，从账号创建、使用到注销进行全流程管理。明确每个阶段的管理要求和责任人，防止账号长期闲置或被恶意利用。

3、定期审查账号权限：定期审查所有远程登录账号的权限设置，确保账号权限与职责相匹配。及时调整不再需要的过高权限账号，降低潜在的安全风险。

4、**账号安全审计：**对远程登录账号的使用情况进行审计和监控。记录账号登录时间、地点、操作等信息，及时发现异常登录行为和潜在的安全威胁。

5、**服务器密码管理：**对云主机的密码进行管理，制定统一的密码策略和变更管理机制，要求运维人员严格执行，并定期进行检查，确保云服务器账号和密码的安全性。

（四）现场监控运维人员操作管理

对运维人员登录云服务器的行为进行监控和管理：

1、**操作规范制定：**制定详细的操作规范和流程，明确运维人员在登录服务器时的要求和注意事项。确保运维人员遵循规范进行操作，减少因不规范操作导致的问题和安全风险。

2、**监控与审计：**实时监控运维人员的操作行为和服务器状态，同时监控上传下载内容，避免出现越权进行数据拷贝等行为。同时，定期审计操作日志和系统事件，检查是否存在违规操作或潜在的安全问题。

（五）网络管理

规划和管理北京市药品监督管理局现有的国家局专网、药监专网、副中心核心网络、政务网，包括但不限于以下内容：

1、路由变更配置

1)、**评估现有网络结构和配置：**对当前使用的网络设备、拓扑结构、路由协议等基础设施进行全面的调查和分析，进行合理的网络规划。利用网络监控工具和流量分析工具，评估网络的实时运行状态和性能瓶颈，提出优化建议。

2)、**制定详细的路由变更方案：**基于业务需求和网络发展趋势，制定详细的路由变更方案。该方案应包括变更目标、变更步骤、风险评估和应对措施等内容。同时，需要充分考虑网络可用性和容灾能力。

3)、**路由变更实施：**根据制定的变更方案，按照步骤逐一进行实施。在实施过程中，要注重团队协作和沟通，确保各个部门之间的协同工作。同时，实时监控网络性能和设备状态，及时发现和解决潜在问题。

4)、验证与测试：在完成路由变更后，进行全面的验证和测试，确保网络正常运行。测试内容包括但不限于连通性测试、路由协议测试、网络安全测试等。

5)、文档化管理：对所有路由变更的过程和结果进行详细记录，形成文档备查。文档应包括变更时间、操作人员、变更内容、测试结果等信息，为今后的网络维护和管理提供参考。

2、策略配置

1) 访问控制策略：根据各部门职责和业务需求，制定合理的访问控制策略。利用身份验证和授权管理机制，确保只有经过授权的用户能够访问相关资源。同时，加强网络设备的安全防护，防止未经授权的访问和攻击。

2) 安全策略：制定全面的网络安全策略，包括防火墙配置、入侵检测与防御、恶意软件防护等内容。定期评估网络安全策略的有效性，并根据业务发展和威胁变化进行更新。

3) 流量控制策略：根据业务需求和网络带宽资源，制定合理的流量控制策略。利用 QoS 技术对网络流量进行分类和优先级管理，确保关键业务的流畅运行。同时，合理规划和管理非关键业务流量，避免带宽资源的浪费和冲突。

3、网络故障解决和管理

1) 故障预防机制：建立完善的故障预防机制，通过定期维护、巡检和监控等手段，及时发现潜在的网络故障和问题。利用日志分析工具和监控平台，实时监测网络设备和应用的运行状态，提高故障预警和快速响应能力。

2) 故障响应流程：制定详细的故障响应流程，明确各个部门和人员的职责和 workflow。建立高效的协作机制，确保在故障发生时能够迅速响应和处理。同时，对故障处理过程进行记录和分析，总结经验教训，提高故障解决效率。

3) 实时解决各种网络故障：要求驻场人员能够实时解决各种网络故障和突发事件，并根据业务需要实时调整网络策略。

4、IP 地址管理

对北京市药品监督管理局全局的 IP 地址进行统一管理和分配：根据业务规模和发展趋势，制定合理的 IP 地址规划方案。确保 IP 地址的唯一性和连续性，遵循 IPv4/IPv6 混合使用的原则，合理分配 IP 地址空间。

（六）维护范围

1、系统硬件

对于本项目清单内明确列明的所有硬件设备，供应商提供自合同签订日起一年的全程维保服务。维保期间涵盖硬件设备的故障检测、维修、更换（非人为损坏）、调试等全流程服务，确保硬件设备正常运转，人为损坏、不可抗力导致的硬件故障除外，相关界定标准另行约定。

2、服务方式及内容

服务内容：覆盖硬件及网络系统全生命周期运维，具体包括：系统定期预防性检查与维护、硬件及网络各类故障的快速响应和彻底修复服务；严格按照北京市药品监督管理局的部署及要求，实施系统硬件升级、PTF 安装调试工作，并同步提供针对性的操作培训、技术指导及咨询服务；在重大活动、关键业务节点等特殊时段，提供专项硬件及网络系统保障服务，确保业务无中断。根据需求，提供涵盖硬件及网络系统使用管理、操作规范、性能优化、风险防控等相关领域全方位技术咨询服务。

服务方式：派驻 2 名专业工程师常驻北京市药品监督管理局指定办公地点，专职负责日常运维服务工作；同时组建不少于 5 人的专项项目团队（含项目经理、技术骨干、备件管理人员）提供全方位技术支撑，确保一线常驻工程师实行主备机制，主岗工程师因故离岗时，备岗工程师需立即补位，保障日常运维服务不中断、不脱节。

3、备机保障及支持体系要求

供应商应针对本项目提供完备的 100%备机备件覆盖保障，供应商应在响应文件中详细说明供应商日常备件保障及支持体系，并提供拟为本项目专门配备的详细备机备件清单，详细说明备件名称、规格型号、数量、存放具体地址（精确

到楼层/库房), 并明确承诺备机备件到达故障现场的具体时间。

4、本项目管理及延伸服务

4.1 供应商应提供针对本项目的服务计划和方案, 说明供应商如何提供满足采购人要求的服务, 该服务计划和方案应包括(但不限于)以下内容:

管理模式及拟为本项目设立的组织机构/管理架构图

工作计划、人员配备、必须的物质装备计划, 及拟投入本项目的主要用品、工具及设备清单;

拟在本项目任职的主要管理人员的简历表及背景资料;

培训计划;

沟通管理;

备件管理;

各项服务指标的承诺及为完成承诺指标采取的具体可落地措施;

4.2 服务档案

对北京市药品监督管理局的所有服务范围内的网络、安全设备等所有设备的系统, 供应商应建立相应的系统维护档案, 并根据每次故障维修报告和预防性维护报告建立技术档案, 记录每次故障响应服务和预防性维护的详细信息(含时间、人员、问题、处理过程、结果、整改建议等)。并协助北京市药品监督管理局做好维保设备档案维护, 确保甲方档案信息与实际服务情况同步更新。

5、其他延伸服务

根据北京市药品监督管理局需要, 在特殊时段(法定节假日、重大活动、突发事件等期间内)提供 7×24 小时现场值守支持服务(至少 1 名资深工程师现场值守), 以及二线技术团队 7×24 小时远程响应服务。

根据北京市药品监督管理局临时需求, 供应商需在 2 小时内将所需现场备件送达指定地点, 配合甲方完成应急保障。

（七）项目团队

1、派驻至少 2 名驻场人员：以现场方式提供服务，驻场期间工作统一由甲方安排、调度与支配，严格遵守甲方规章制度。

两名驻场人员均须满足以下条件：

1)、计算机相关专业，从事**服务器及网络设备相关技术工作 10 年及以上**，具备丰富的机房运维、设备实施与故障处置经验；

2)、精通主流服务器、存储等硬件安装、配置、巡检与故障排查；

3)、精通交换机、路由器、防火墙等网络设备调试、策略配置、链路优化及故障定位；

4)、具备系统安全加固、应急响应、突发事件处理及运维文档编写能力。

其中 1 名驻场工程师须额外具备云服务器管理技能，熟练掌握公有云 / 私有云服务器部署、配置、运维、监控、安全加固及故障处理。

2、配备 1 名项目技术负责人：需在供应商本单位从业 8 年（含）以上，并同时具备有效的信息系统项目管理师（高级）证书。负责本项目的项目管理，统筹相关工作，项目监督与情况汇报，控制工作质量和预算，执行变更和应急情况管理，并根据实际状况调整供应商人员安排，以保证此项目的正常高效运作。

3、配备不少于 5 名一线工程师，并具备有效的注册信息安全专业人员（CISP）认证证书。

4、配备不少于 2 名二线工程师，且需在供应商本单位从业 8 年（含）以上，并具备有效的注册信息安全专业人员（CISP）认证证书、计算机技术与软件专业技术资格网络工程师证书。