



甲方合同编号：【 】

乙方合同编号：【 】

河南移动【漯河】分公司与【漯河市源汇区卫生健康委员会】关于【漯河市源汇区卫生健康委员会源汇区妇幼保健院能力提升建设】项目合作协议

本范本适用于 ICT 业务销售合同（设备销售+集成+维保），并融合移动云业务和互联网专线业务）

甲方：【漯河市源汇区卫生健康委员会】（盖章）

法定代表人：

住所：

授权代表签字：

电话：

联系人：

乙方：【中国移动通信集团河南有限公司漯河分公司】（盖章）

负责人：

住所：

授权代表签字：

电话：

联系人：

合同签订日期 2025 年 3 月 17 日





根据《中华人民共和国民法典》、《中华人民共和国电信条例》及其他有关法律、法规的规定，在平等、自愿、公平、诚实、信用的基础上，双方就漯河市源汇区卫生健康委员会源汇区妇幼保健院能力提升建设项目有关事宜协商一致，达成合同如下：

第一条 合作内容

1.1 乙方在现有技术条件下、现有网络覆盖范围内，为甲方有偿提供【漯河市源汇区卫生健康委员会源汇区妇幼保健院能力提升建设】项目设备销售，以及对应的集成、维保服务、云主机服务。

1.2 乙方为甲方提供的具体服务内容及要求详见【附件 1：设备清单及技术规范】。乙方为甲方提供的【云主机服务】除遵守本合同正文约定外，双方同时按照相应附件中的约定执行。

第二条 资费标准和支付方式

2.1 本合同项下甲方应当向乙方支付的合同款项包括设备采购费、集成服务费、维保服务费、云主机服务费等。

2.2 本合同项下甲方应当向乙方支付的合同款项（含税）共计【2565000】元（大写：人民币贰佰伍拾陆万伍仟元整），详见下表。

项目名称	合同内容	未含税总价 (元)	税率(%)	增值税税额 (元)	含税总价 (元)
漯河市源汇区卫生健康委员会源汇区妇幼保健院能力提升建设项目	云主机服务费	3118.87	6	187.13	3306.00
	ICT 设备销售费	919955.75	13	119594.25	1039550.00
	ICT-云计算-集成费	1342022.64	6	80521.36	1422544.00
	ICT-云计算-维保费	93962.26	6	5637.74	99600.00
合计		2359059.52	/	205940.48	2565000.00

2.3 合同项下所有款项由甲方向乙方以如下方式及比例支付：

【第一笔付款：甲乙双方签订合同起 10 个工作日内，甲方向乙方支付合同总价款的 30%作为预付款，即 769500 元（含税）（大写金额：人民币柒拾陆万玖仟伍佰元整）。

第二笔付款：项目建设所需设备到货，甲乙双方开箱检验无误后，并签署开箱检验合格证书起 10 个工作日内，甲方向乙方支付合同总价款的 40%，即 1026000 元（含税）（大写金额：人民币壹佰零贰万陆仟元整）。

第三笔付款：甲乙双方对项目成果进行验收，各项功能及指标符合合同约定要求的，甲乙双方



第四笔付款：甲乙双方签订签署项目验收合格报告 12 个月后 10 个工作日内，甲方向乙方支付合同总价款的 3%，即 76950 元（含税）（大写金额：人民币柒万陆仟玖佰伍拾元整）。】

任何一方如需改变上述账户信息（乙方名称和纳税人识别号不可改变），应在变更账户前十（10）日以书面通知另一方并征得对方同意。如一方未按本合同约定单独变更账户信息而使另一方遭受损失的，应予以赔偿。

2.7 在甲方支付本合同项下的综合服务费之前,乙方应当向甲方开具相应金额的增值税【普通】(普通/专用)发票。

自项目验收通过之日起乙方为甲方提供维保服务，维保期为【1】年。

第四条 设备验收、集成验收





4.1 设备验收

4.1.1 甲方指定的地点及收货人：【 河南省漯河市 】。

4.1.2 开箱检验在乙方将货物运送至甲方指定交货地点后【7】日内进行，双方根据合同约定检查货物，检验后无任何问题的签署开箱检验合格证书。

4.2 集成验收

4.2.1 根据中华人民共和国国家和履约地相关质量标准、行业技术规范标准、采购文件的要求及乙方的响应承诺验收。

4.2.2 在乙方完成集成服务 7 个工作日内，双方应对项目成果进行验收，各项功能及指标符合要求的，由双方签署项目验收合格报告。

4.3 甲方自收到乙方提交的验收申请后 7 个工作日内未组织验收，且自乙方催告后 3 个工作日内仍未组织验收的，视为验收通过。

第五条 售后服务

乙方维保具体内容如下：



5.1 为保证系统正常运行所需的预防性维护、日常维护支持、网络调整支持、数据备份支持等工作。

5.2 提供每周 7 天每天 24 小时的技术支持服务。如果出现紧急技术问题，在甲方通过电话或传真通知乙方的情况下，乙方的工程师应在 1 小时内予以答复。如果甲方要求紧急处理，乙方应在收到甲方通知后的 4 小时内赶到现场。当合同系统提供的业务中断时，乙方在提供远端服务的同时，须在收到甲方通知后 2 小时内赶到现场，因不可抗力致使乙方未按时到达现场的除外。

5.3 硬件设备发生损坏的，若在质保期内，设备维修或更换的成本由乙方承担（因甲方故意或使用不当导致设备损坏的除外）；若在质保期外，设备维修或更换的成本由甲方承担。

第六条 双方的权利与义务

6.1 甲方的权利和义务

6.1.1 在本合同有效期内，甲方有权要求乙方根据本合同约定和产品使用说明书的描述向甲方提供相应的产品和服务。

6.1.2 甲方同意，乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

6.1.3 甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

6.1.4 甲方承诺并保证不利用乙方提供的设备或服务进行任何违反国家政策法律法规、侵犯乙方或第三方合法权益的行为，否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。





6.1.5 甲方应本合同的约定，及时足额向乙方支付各项费用。

6.1.6 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

6.1.7 甲方使用乙方提供的本合同约定产品或服务时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品或服务的，相关责任由甲方承担。

6.1.8 甲方成为乙方集团客户后，如果乙方提供了服务账号，甲方应妥善保管乙方提供的相关服务账号和甲方设定的服务密码。服务账号和密码是甲方办理产品相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。甲方应当承担因账号和密码保管不善产生的费用。

6.1.9 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将产品或服务提供给甲方，甲方承担由此造成的责任和后果。

6.1.10 甲方负责系统建设验收后的后期维护工作，本合同另有约定的除外。

6.1.11 未经乙方同意，甲方不得将乙方的软件、技术、设施、设备等用于双方合作项目以外的其他用途，且不得向第三方透漏、转让。若甲方违反本条款，乙方有权要求甲方赔偿损失，撤回设备、终止协议。

6.1.12 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失。

6.2 乙方的权利和义务

6.2.1 乙方应按合同约定向甲方提供相关硬件设备，并完成系统集成、维护等工作。乙方人员应携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

6.2.2 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定产品或服务的，应提前通知甲方，甲方应给予必要的配合。

6.2.3 乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

6.2.4 在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

6.2.5 因第三方实施破坏、网络攻击等非乙方原因导致甲方不能正常使用乙方产品和服务的，不视为乙方违约，乙方不承担相应责任。

6.2.6 乙方有权本合同约定要求甲方及时足额支付各项费用。

6.2.7 乙方应对其所委托的代为向甲方提供本合同项下服务的第三方的服务行为向甲方承担责





任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

6.2.8 因甲方员工与乙方存在电信服务合同关系，若在本合同履行过程中，甲方员工就与本合同有关的服务提出异议时，为保证甲方员工利益，乙方有权对提出异议的甲方员工暂停提供与本合同有关的甲方员工个人服务，并由三方进行协商。待三方意见一致时，再向提出异议的甲方恢复本合同服务，乙方无需因此向甲方承担违约责任。甲方员工如对已经提供的服务要求乙方承担责任时，该责任由甲方向乙方承担。

第七条 保密条款

7.1 “保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接受方”）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于：技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接受方及其人员为本协议目而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。甲方理解并同意，乙方及其关联公司可通过业务受理系统登记、纸质档案，通过网络接收、读取并记录等方式，以提供电信服务为目的，在业务活动中收集、使用甲方提供的和甲方使用服务过程中形成的信息。乙方有权依法对包含甲方在内的整体用户数据进行分析并加以利用。未经甲方同意，乙方不向除乙方关联公司外的第三方提供甲方信息。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

7.3 双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；同时，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

7.4 接受方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接受方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。接受方向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

7.5 如相关政府部门或监管机构要求接受方披露任何保密信息，接受方可在该政府部门或机构要求的范围内做出披露而无需承担本协议项下的保密责任。但前提是，该接受方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接受方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。





7.6 双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性以及对甲乙双方的约束力。

7.7 由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

7.8 在任何情形下，本合同约定的保密义务应永久持续有效。

第八条 违约责任

8.1 甲方未按照本合同约定的期限支付合同款项的，从逾期的次日起计算违约金，每滞后 1 天支付合同未付金额的【3%】的违约金，违约金总额超过合同金额的【20%】时，乙方有权解除本合同，并保留进一步追偿的权利。

因乙方原因导致乙方未按照本合同约定时间完成项目的，每逾期一天应向甲方支付合同金额 1% 的违约金。

8.2 如甲方未按本合同约定或国家法律法规规定及时办理相关备案或审批手续，因此产生的一切责任和后果均由甲方承担。根据国家法律法规、通信管理部门的规定或通知，乙方有权中断、终止为甲方提供本协议项下的全部或部分业务，且无需承担任何违约责任。

8.3 乙方在进行网络调整和维护时需要短时间中断服务，或者由于 Internet 上骨干网通路的阻塞造成甲方服务器访问速度下降，甲方认同属于正常情况，不视为乙方违约。

8.4 下列情况下乙方有权单方终止本合同，并停止向甲方提供服务。由此给甲方造成的损失，乙方不承担责任，并有权要求甲方承担违约或赔偿责任：

- (1) 甲方（包括联系人）提供虚假证照的；
- (2) 甲方利用乙方提供的产品和服务实施违反国家法律、法规 and 政策的；
- (3) 甲方利用乙方提供的产品和服务从事其他不当用途（如：甲方将乙方提供用于本合同业务的相关设备转售、转租、转借第三方，或将乙方提供的设备、产品和服务接入其他通信服务提供商的业务）或侵犯第三方的合法权利；
- (4) 乙方根据国家有关部门的要求停止为甲方提供相关服务；
- (5) 甲方所使用的所有产品和服务中有一项产品欠费超过三个月，或有二项以上产品欠费均超过一个月。

8.5 乙方仅对因其过错给甲方造成的直接损害结果承担赔偿责任，且不包括第三方提出的索赔要求、数据丢失或损坏的损失，不包括经营损失等一切间接损失。无论何种情况，乙方对本协议项下的违约赔偿总额不超过本协议项下已支付的服务费用的总和。

第九条 不可抗力及免责条款

9.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

9.2 由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能





按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：（1）受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五（15）天内提供有关该事件的公证文书和书面说明，书面说明中应包括对迟延履行或部分履行本合同的原因说明。

9.3 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

9.4 如果不可抗力事件的影响持续达三十（30）日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十（10）日内双方无法就此达成一致，任何一方均有权解除本合同而无需承担违约责任。

9.5 乙方对下述事项不承担责任：（1）第三方对甲方提出的索赔要求；（2）甲方的记录或数据的丢失或损坏；（3）甲方的经营损失等一切间接损失。

9.6 如因乙方难以避免、难以排除的技术或网络故障或第三方原因造成甲方无法使用本协议项下服务的，不视为乙方违约，但乙方应尽合理努力争取在最短时间内解决，对此双方无异议。鉴于计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方亦认同不属于乙方违约。

第十条 通知与送达

10.1 根据本合同需要发出的全部通知，均须采取书面形式，对本合同效力产生影响的、或解决合同争议时的通知或函件，以（A）专人递送，（B）特快专递发出。特快专递的交寄日以邮戳为准。上述书面通知均须标明合同对方为收件人。

10.2 上述书面通知按对方在本合同通知与送达条款中所列的地址发出。如双方中任何一方的地址有变更时，须在变更前十日以书面形式通知对方，因延迟通知而造成的损失，由延迟通知方承担责任。

10.3 双方将按如下约定确定通知送达完成时间：

10.3.1 以专人递送的，接收人签收之日视为送达；

10.3.2 以特快专递形式发出的，发往本市内的，发出后第【3】日视为送达。发往国内其他地区的，发出后第【5】日视为送达；

10.3.3 以特快专递形式发出的通知，必须向本合同通知与送达条款约定的地址或者依据本合同变更后的地址发出；任何一方未按照本合同约定的送达方式送达的，视为未履行通知送达义务；

10.3.4 以电子邮箱形式发出的，到达接收人电子邮箱所在系统之时视为送达；

10.3.5 以电子邮箱形式发出的通知，必须向本合同约定的电子邮箱发出；任何一方未按照本合同约定的电子邮箱送达的，视为未履行通知送达义务；





10.3.6 合同各方均明知：因各方提供或者确认的通信地址和联系方式不准确、或者通信地址变更后未及时依程序告知对方和司法机关、或者当事人和指定接收人拒绝签收等原因，导致商业信函、诉讼文书等未能被当事人实际接收，以专人递送的，送达至通知与送达条款约定的地址之日即视为送达之日；以特快专递形式发出的，按照通知与送达条款约定的方式确定送达之日。

各方地址与联系方式如下：

甲方：【漯河市源汇区卫生健康委员会】

地址：【漯河市源汇区建新路 14 号】

电话：【0395-5759001】

电子邮件：【/】

邮政编码：【462000】

乙方：【中国移动通信集团河南有限公司漯河分公司】

地址：【漯河市湘江东路 23 号】

电话：【0395-2639000】

电子邮件：【/】

邮政编码：【462000】

第十一条 争议解决

11.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

11.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。

11.3 如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则如果双方通过协商不能解决争议，则双方同意向乙方住所地人民法院提起诉讼。

11.4 诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。本合同全部或部分无效的，争议解决条款依然有效。

第十二条 其他约定

12.1 本合同一式【肆】份，双方各持【贰】份，具有同等法律效力。

12.2 对于合同未尽事宜、双方可签订补充合同对本合同中的问题做出补充、说明、解释。本合同的补充合同作为本合同不可分割的一部分，与本合同具有同等的法律效力。

12.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

12.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前 30 日向另一方提交书面说明。单方面解除协议的一方，

12.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前 30 日向另一方提交书面说明。单方面解除协议的一方，





应对另一方因此遭受的损失承担全部赔偿责任。

第十三条 本合同附件

附件 1：设备清单及技术规范

附件 2：网络与信息安全协议书

附件 3：移动云 IaaS 业务服务条款（作为 ICT 融云合同的附件）（云主机服务协议）

（以下无正文）



河南移动 合同管理



河南移动 合同管理





附件 1:

设备清单及技术规范

一、项目技术规范总体概述

随着信息技术的飞速发展，医院作为重要的医疗服务机构，面临着提升服务质量和效率、保障患者隐私安全、优化医疗流程等多重挑战。为了应对这些挑战，妇幼保健院决定实施信息化改造项目，通过引入先进的信息化技术和设备，全面提升医院的信息化水平和服务能力。

本项目旨在通过信息化改造，实现以下目标：

提升医疗服务质量和效率，为患者提供便捷、高效的医疗服务。

加强医院信息安全防护，保障患者隐私和数据安全。

优化医疗流程，减少人为错误和等待时间，提高患者满意度。

建立完善的信息化管理体系，为医院的可持续发展奠定坚实基础。

二、设备清单

序号	类型	采购名称	技术参数	数量	单位	税率	含税单价	含税总价
1	ICT 设备 销售	内外网隔离网闸	1. 提供标准 2U 机架式设备，采用“双主机+隔离卡”架构； 2. 内存 16GB，硬盘 960G SSD，配置冗余电源，内外网各 6 电口； 3. 整机吞吐量 300Mbps，并发连接数 10W； 4. 基于硬件隔离开关实现内外网络物理断开； 5. 支持 HTTP 应用改写功能，能适应各种不同 Web 应用场景； 6. 支持基于 TCP、UDP 协议的非标准应用协议以及 IP、SMTP、POP3、MULTICAST、网络协议等； 7. 支持国际主流视频控制协议 SIP、RTMP、GB28181；	1	台	13%	85300	85300



		8. 支持对客户端 IP、端口、访问时间、命令的检查过滤功能; 9. 支持自带的防病毒能对来往应用数据进行病毒查杀; (提供产品功能截图并加盖厂商公章) 10. 支持与第三方日志系统对接, 实现基于 syslog 的日志推送; 11. 支持基于五元组 (源地址、源端口、目的地址、目的端口、协议) 的访问控制机制; 12. 外网端不允许配置管理接口, 所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置; 13. 含三年授权升级与产品质保服务。					
	超融合硬件平台	1. 提供标准 2U 机架式服务器, 含上架导轨等配件; 2. CPU: 2 颗 16 核 intel Xeon Silver 4314, 主频: 2.4GHz; 3. 内存: 8*32GB DDR4 3200; 4. 标配盘位数: 12 个, 满配硬盘托架; 5. 系统盘: 2*240GB SATA SSD; 6. 缓存盘: 2*1.92T SATA SSD, 数据盘: 3*10T 机械硬盘; 7. 接口: 提供 4 千兆电口+4 万兆光口; 8. 电源: 提供白金, 冗余电源。	4	台	13%	76576	306304
3	超融合组网交换机	1. 交换容量 2. 56Tbps/23.04Tbps 2. 包转发率 456Mpps 3. 固定端口: 提供 24 个	2	台	13%	12000	24000



		千兆 SFP 端口, 28 个 10G SFP+ 端口, 支持全端 口线速转发, 支持统一管 理 4. 支持丰富的业务特性、 完善的安全控制策略、丰 富的 QoS 等特性; 交换机 深度 220mm, 采用电源前 置设计; 5. 含三年授权升级与产 品质保服务。					
4	服务器	1. 提供标准 2U 机架式设 备, 含上架导轨; 2. CPU2 颗 intel 至强可 扩展系列处理器 4210; 3. 内存 128GB DDR4; 硬 盘 3 块 4T SATA 硬盘; 4. 含一年授权升级与产 品质保服务。	3	台	13%	29800	89400
5	等保 一体 机硬 件平 台	1. 提供标准 2U 机架式设 备, 含上架导轨; 2. CPU2 颗 16 核 intel Xeon Silver 4314, 主频 2.4GHz; 3. 内存 4*32GB DDR4 3200, 系统盘 2*480GB SSD, 缓存盘 2*480GB SSD, 数据盘 2*6T 机械硬盘, 标配盘位数 12 个, 标配 白金冗余电源, 接口 4 千 兆电口+2 万兆光口; 4. 支持网桥、路由、旁路 模式部署; 5. ★等保一体机硬件平 台内置 1 套管理软件, 开 箱即用, 无需二次安装, 平台必须能够根据授权 数量按需创建虚拟下 代防火墙、虚拟上网行为 管理、虚拟 SSL VPN、虚 拟负载均衡、虚拟数据库 审计、虚拟运维安全管 理、虚拟日志审计、虚拟 云镜脆弱性扫描、终端安	1	台	13%	46522	46522



		全检测与响应、云主机安全保护等独立的安全组件，还能够集成第三方生态产品以扩充平台安全能力。（需提供产品界面截图，并加盖厂商公章） 6. 支持在首页整体展示全部业务系统的风险状态，包括业务风险分布、安全事件列表（包括失陷事件、攻击事件和漏洞事件）等。 7. 平台侧界面必须支持监测等保一体机资源状态（包括总计算资源、总内存资源及总存储资源）和系统预警，系统预警能够体现告警主机、告警应用、待处理事件。 8. 平台侧界面支持安全组件分配功能，管理员可直接为各个分配安全资源，同时完成关键安全资源的策略初始化。（需提供产品界面截图，并加盖厂商公章） 9. 含三年硬件质保与售后技术支持服务。					
6	上网行为管理	1. 提供标准 1U 机架式设备，内存 4G，硬盘容量 128G SSD，标配单电源，接口 6 千兆电口+2 千兆光口 SFP； 2. 整机吞吐量 3Gb，带宽性能 200Mb，支持用户数 1000，最大并发连接数 120000； 3. 支持路由模式、网桥模式、旁路模式； 4. ★支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名、资产类型分布、新设备发现趋势、终	1	台	13%	48000	48000



	端违规检查项排行、终端违规用户排行等：（提供产品功能截图并加盖厂商公章） 5. 支持权限策略故障排查，支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略；权限策略故障排查； 6. 支持首页分析显示接入用户人数、终端类型；实时流量排名资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行； 7. 支持通过抑制 P2P 的下行丢包，来减缓 P2P 的并行流量，从而解决网络出口在做流控后仍然压力较大的问题； 8. 支持记录全部或者指定类别 URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能：（提供产品功能截图并加盖厂商公章） 9. 支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行识别； 10. 支持图形化查看内网 IP 使用情况，帮助管理员减少维护 IP 表的工作量； 11. ★支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级：（提供产品功能截图并加盖厂商公章）； 12. 支持针对特权用户配置免认证 key、免审计 key、免控制 key； 13. 含三年授权升级与品质质保服务。				
--	---	--	--	--	--



7	外网 防火 墙	1. 提供标准 1U 机架式设备，内存 4G，硬盘容量 128G SSD，标配单电源，接口 8 千兆电口+2 千兆光口 SFP； 2. 整机吞吐量 4G，IPS 吞吐量 600M，HTTP 新建连接数 6 万，并发连接数 200 万，IPSec VPN 吞吐量 270M； 3. 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等部署方式； 4. 支持 IPv4/IPv6 双栈工作模式； 5. 支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略； 6. 支持僵尸主机检测功能，产品内置僵尸网络特征库超过 120 万种，可识别主机的异常外联行为； 7. ★支持服务器漏洞扫描功能，并对扫描源 IP 进行日志记录和联动封锁；（提供具有 CNAS/CMA 资质的第三方机构的检测报告） 8. 支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改；（提供具有 CNAS/CMA 资质的第三方机构的检测报告） 9. 支持多种 SSL VPN 用户认证方式，至少包括本地密码认证、LDAP 认证和硬件特征码认证，提供 20 个 SSL VPN 接入授权； 10. ★支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；	1	台	13%	45000	45000
---	---------------	---	---	---	-----	-------	-------



	(提供具有 CNAS/CMA 资质的第三方机构的检测报告) 11. ★支持联动云端智能运营平台, 支持流量日志分析、事件聚合、云端专家研判, 安全事件微信端就可接受预警和处置; (提供产品功能截图证明并提供官方机构针对该功能的检测证明) 12. 支持杀毒白名单设置, 可以例外排除特定 MD5 和 URL 的病毒文件, 针对特定文件不进行查杀; 13. 含三年授权升级与产						
	内网数据库审计 1. 提供标准 1U 机架式设备, 内存 8G, 硬盘容量 2T, 标配单电源, 接口 6 千兆电口+2 万兆光口 SFP+; 2. 整机吞吐量 2Gbps, 数据库流量 400Mb/s, 数据库实例个数 30 个, SQL 处理性能 30000 条 SQL/s, 日志检索性能 500000 条/秒; 3. 提供旁路接入模式, 设备部署不影响原有网络结构; 4. 采用 B/S 管理方式, 无需在被审计系统上安装任何代理; 无需单独的数据库中心, 一台设备完成所有工作; 5. 支持同时审计多种数据库及跨多种数据库平台操作; 6. ★支持通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表, 帮助用户提升通过高级	1	台	13%	95000	95000	



		选项筛选报表的可读性，更方便达到预期效果； （提供产品功能截图并加盖厂商公章） 7. 支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险排行； 8. 支持基于 SQL 命令的 webshell 检测； 9. ★支持查看正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统等信息； （提供产品功能截图并加盖厂商公章） 10. 支持导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息等安全规则； 11. 支持 TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询； 12. 支持通过 SQL 串模式抽取保障磁盘 IO 的读写性能； 13. 含三年授权升级与产品质保服务。					
9	内网准入控制	1. 提供标准 1U 机架式设备，内存 4G，硬盘容量 128G SSD，标配单电源，接口 6 千兆电口+2 千兆光口 SFP； 2. 吞吐量 3Gb，最大并发连接数 120000，准入终端授权数 500； 3. 支持路由模式、网桥模式、旁路模式；	1	台	13%	60000	60000



		4. 支持 Windows 终端安全检查，包括杀软检查、进程检查、补丁检查等； 5. 无需安装客户端，通过流量状况检查主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复； 6. 支持 Windows 终端调用管理员上传脚本/程序以满足个性化检查要求，可设置周期性运行或者运行一次；（提供产品功能截图并加盖厂商公章） 7. 支持 Windows 桌面水印，支持设置水印的内容、透明度、密度，水印效果预览，离线时继续生效；（提供产品功能截图并加盖厂商公章） 8. 支持放通或封堵 TCP\UDP 端口、ICMP 协议，可设置对所有 IP 或者指定 IP 执行，离线时继续生效； 9. ★支持对终端应用联网管控，可设置禁止或允许访问互联网，禁止或允许访问指定 IP 地址，离线时继续生效；（提供产品功能截图并加盖厂商公章）； 10. ★支持对 U 盘、移动硬盘设置可读写、拒绝、可读、告警；可对拷贝的文件内容以及插入和拔出行为的审计。（提供产品功能截图并加盖厂商公章）； 11. 含三年授权升级与产品质保服务。					
10	内网防火墙	1. 提供标准 1U 机架式设备，内存 4G，硬盘容量 128G SSD，标配单电源，	1	台	13%	45000	45000



	接口 8 千兆电口+2 千兆光口 SFP; 2. 整机吞吐量 4G, 应用层吞吐量 2G, 防病毒吞吐量 600M, 并发连接数 200 万, HTTP 新建连接数 6 万; 3. 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等部署方式; 4. 支持 IPv4/IPv6 双栈工作模式; 5. 支持基于网络区域、网络对象、MAC 地址、服务、应用、域名等维度进行访问控制策略设置; 6. 支持对压缩病毒文件进行检测和拦截, 压缩层数支持 15 层; (提供产品功能截图并加盖厂商公章) 7. ★具备独立的勒索病毒防护模块, 非普通防病毒功能, 支持对特定的业务进行勒索风险自动化评估, 并依据评估结果自动生成防护策略; (提供关于“勒索病毒”的软件著作权证明功能有效性) 8. 支持僵尸主机检测功能, 产品内置僵尸网络特征库超过 120 万种, 可识别主机的异常外联行为; (提供具有 CMA/CNAS 资质的第三方机构的检测报告) 9. ★支持服务器漏洞扫描功能, 并对扫描源 IP 进行日志记录和联动封锁; (提供具有 CMA/CNAS 资质的第三方机构的检测报告) 10. 支持 Cookie 攻击防护功能, 并通过日志记录 Cookie 被篡改;				
--	--	--	--	--	--



	11. 支持对跨站脚本 (XSS) 攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护; 12. 支持 X-Forwarded-For 字段检测, 并对非法源 IP 记录和联动封锁; 13. 支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护; 14. 含三年授权升级与产品质保服务。					
11	核心交换机 1. 交换容量 76.8Tbps, 包转发率 57600Mpps, 主控引擎 2; 整机业务板槽位数 6 适用 600mm 深度机柜; 2. 安全自主可控, CPU 和交换等芯片采用国产化芯片, 提供第三方测试报告; 3. 设备支持模块化风扇框, 可热插拔, 独立风扇框数 2 个, 支持颗粒化电源, 整机电源槽位数 4 个, 可在机柜内并排部署, 设备机箱 (包括业务板卡区) 采用后出风风道设计; 4. 整机 MAC 地址为 384K; 支持 4K VLAN; 5. IP 路由 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议, 支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议; 6. 支持 MPLS 基本功能; 支持 MPLS OAM 支持 MPLS TE 支持 MPLS VPN/VLL/VPLS;	2	台	13%	85000	170000



12	光模块	7. 管理运维：支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理，支持 Telemetry 技术，实时采集设备数据并上送至网络分析组件平台，通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，及时定界故障以及故障发生原因，精准保障用户体验； 8. 双主控，双电源，万兆光口 24 个，千兆光口 24 个，千兆电口 48 个，1 条万兆堆叠线缆； 9. 含三年授权升级与产品质保服务。	50	只	13%	457	22850
		提供 LC-LC 万兆多模双纤条线 30 根，长度 3M-10M 不等，根据现场情况定制。六类国标纯无氧铜网线，六类水晶头一盒。	1	项	13%	2174	2174
		提供 LC-LC 万兆多模双纤条线 30 根，长度 3M-10M 不等，根据现场情况定制。六类国标纯无氧铜网线，六类水晶头一盒。	1	项	13%	2174	2174
14	ICT-云计算-集成服务	超融合软件平台 1. ★超融合软件和超融合服务器为同一品牌，提供一体化交付； 2. 配置 8 颗 CPU 的超融合软件授权，超融合软件包含 CPU 计算虚拟化、存储虚拟化、网络虚拟化和云计算管理软件授权，且为同一品牌并完全自主研发； 3. 提供 1 套持续数据保护 CDP 软件，包含 20 个虚拟化授权； 4. 提供 8 颗 CPU 安全虚拟化授权，安全虚拟化 unlimited 虚拟机防护数量； 5. 支持虚拟机卡死及蓝	1	项	6%	535000	535000



		屏的检测功能并实现自动重启，无需人工干预； 6. 支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险； 7. 持续数据保护软件模块采用无代理的方案，避免对虚拟机的稳定性和性能产生影响，可设置RPO为5秒或1秒； 8. ★支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道；（提供具有CNAS/CMA资质的第三方机构的检测报告） 9. 在管理平台上可以通过拖拽连线完成网络拓扑的构建，可以在网络拓扑页面通过功能键实现虚拟网络连接、开启和关闭等操作；（提供产品功能截图并加盖厂商公章） 10. ★提供创建疑似勒索快照任务功能，检测到资产防护组件异常、疑似中勒索病毒时，自动触发快照；（提供具有CNAS/CMA资质的第三方机构的检测报告） 11. 云平台具备虚拟补丁能力，无需在主机操作系统打补丁，能直接在网络层对指定虚拟机和批量虚拟机开启虚拟补丁防护；（提供产品功能截图并加盖厂商公章） 12. 支持提供可靠向导化勒索病毒处理流程，包括紧急隔离、保留当前状				
--	--	--	--	--	--	--



			态、恢复云主机、扫描病毒、恢复网络。 13. ★支持跨物理主机的虚拟机 USB 映射, 可进行虚拟机 USB 映射操作; (提供具有 CNAS/CMA 资质的第三方机构的检测报告) 14. 支持创建分布式虚拟防火墙, 可基于虚拟机、虚拟机组、虚拟机标签、IP、IP 范围、IP 组构建安全防火墙。					
15		终端安全管理系统	1. 产品以纯软件交付, 包含管理控制中心及终端安全管理软件授权; 2. 配置 PC 终端授权点数 200 点, 服务器端授权点数 10 点; 3. 采用 B/S 架构的管理控制中心, 具备终端安全可视, 终端统一管理, 统一威胁处置, 统一漏洞修复, 威胁响应处置, 日志记录与查询等功能; 4. 支持终端自动分组管理, 新接入终端可以根据网段自动分配到对应分组; 5. 支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描, 及时发现尚未纳入管控的终端; 6. 支持终端客户端软件的启用禁用, 统一重启和卸载客户端软件; 7. 支持安全策略一体化配置, 通过单一策略可实现不同安全功能的配置; 8. ★支持基于勒索病毒攻击过程, 展示勒索病毒处置情况, 对勒索病毒及变种实现专门有效防御; (提供产品功能截图并	1	项	6%	43478	43478



		加盖厂商公章) 9. 支持监控诱饵文件，当勒索病毒对文件修改或加密操作时进行拦截； 10. 支持全网风险展示，包括但不限于未处理的勒索事件数量、高级威胁、Web 入侵、待处置漏洞、钓鱼攻击及其各自影响的终端数量； 11. 支持禁止黑客工具启动，可以防止黑客攻击； 12. 含三年授权升级与软件技术服务。					
16 	等保一体机软件平台	1. 提供内置 50 个资产的日志审计授权，对每个日志源设置过滤条件规则，自动过滤无用日志。 2. 日志审计功能支持事件详情中字段作为查询条件进行二次检索分析； 3. 支持从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段；（提供产品功能截图并加盖厂商公章） 4. 提供内置 10 个资产的堡垒机运维审计授权； 5. 堡垒机功能授权支持运维水印、录像水印、监控水印开启； 6. 堡垒机功能授权内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色； 7. 提供内置漏洞扫描能力，其中系统漏扫授权 IP 数 50 个； 8. 漏洞扫描支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB	1	项	6%	191600	191600



			漏洞扫描、基线配置核查六种任务类型； 9. 平台可根据实际业务环境定义业务安全区域，简化运维管理；（提供产品功能截图并加盖厂商公章） 10. 支持通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备；（提供产品功能截图并加盖厂商公章） 11. 支持双因素认证功能，用户需在登录时进行双重认证，提高用户的安全性； 12. ★支持基于一体化平台安全管理中心功能，能够对设备进行统一纳管，包括规则库与补丁包统一升级、策略的统一配置、客户端补丁包统一升级等；（提供产品功能截图并加盖厂商公章） 13. 支持禁用默认超级管理员账号，防止特权账号被滥用； 14. 支持基于一体化平台的安全运营中心功能，至少能够提供业务、用户视角的安全风险展示。（提供产品功能截图并加盖厂商公章） 15. 含三年授权升级与软件技术服务。					
17		智能安全驾驶舱	1. 提供1年云端服务，无需在数据中心进行任何下载和安装。 2. 支持不同安全视角展示7个独立的大屏展示功能，包括全网安全能力	1	项	6%	100000	100000



		监控大屏、安全运维大屏、告警态势大屏、资产态势大屏等；（提供产品功能截图并加盖厂商公章） 3. ★全网安全能力监控大屏支持展示网端数据源展示，并支持跳转相关日志检索页面。可直观展示日志到告警，告警到事件的消减比例；（提供产品功能截图并加盖厂商公章） 4. 支持采集网络侧遥测数据，包括脆弱性、服务探测、主机探测、网站攻击、后门通信、账号爆破、攻击利用、邮件攻击、DOS攻击、漏洞利用、黑客工具、异常流量等；（提供产品功能截图并加盖厂商公章） 5. 支持终端防护遥测数据采集：包含传统杀毒类日志、IOA 类日志； 6. ★支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议，支持通过安全 GPT 在线解读事件；（提供产品功能截图并加盖厂商公章） 7. ★支持用户基于安全告警页面入口对安全告警的举证进行解读，以自然语言的方式对告警的内容进行解读，同时支持对安全告警的解读内容进行多轮追问解答；（提供产品功能截图并加盖厂商公章） 8. 支持对资产进行漏洞排查，并将存在特定漏洞资产与相关字段关联起				
--	--	---	--	--	--	--



			来; 9. 支持在对话框当中查询安全事件的列表、并能够根据事件的危害等级进行排查整理; 10. 支持平台上的专业词汇、能够覆盖当前平台页面上专业名词和解读。					
18		体检接口功能模块	1. 实现体检系统内微信、支付宝支付, 微信问卷, 预约及查询体检报告; 2. 现金、体检卡、计帐结算等, 并可与会员管理系统无缝连接实现直接刷会员卡收费支持打折, 多种收费方式; 3. 支持自费、公费、自动补差等, 支持按人员结算、按项目结算、预结、迟结、禁检、结算分析、项目构成等; 4. 微信扫码可查看电子导检单, 查询所有项目及已检情况; 5. 根据身份证号自动关联档案, 可自动生成历届对比报告; 6. 同时提供电子发票对接服务; 7. 中心现有设备对接; 8. 历史数据保留, 支持查询及报告打印。	1	项	6%	160000	160000
19		国家医保接口系统改造	1. 医保明细审核事前分析: 实现门诊医生站、住院医生站开立医嘱信息违规行为、违规明细、违规金额、严重程度等及时核查提醒。 2. 医保明细审核事中分析: 实现门诊预结算、住院预结算对已上传明细费用行整体违规行为、违规明细、违规金额、严重程度等核查提醒。	1	项	6%	82466	82466



20		云主机服务	1. CPU4核, 内存 8G, 云硬盘 200G; 2. 提供接入公网带宽 5Mbps; 3. 云主机提供主流的 Windows 等操作系统, 具备正版授权。	1	年	6%	3306	3306
21		等保测评服务	为医院 HIS、LIS、PACS、EMR 系统提供等保测评服务	1	项	6%	100000	100000
22		系统集成服务	提供整体的安装调试及软硬件、网络对接服务	1	项	6%	210000	210000
23	ICT-云计算-运维服务	安全托管服务	1. 每月提供 3 次现场巡检服务, 巡检项包括物理环境、网络环境、安全设备及网络设备、服务器告警处理; 设备版本升级及规则库更新服务、服务器漏洞更新及终端病毒查杀及处理, 针对病毒文件提供沙箱检查服务; 2. 全年无休 7*24 小时现场应急响应, 不限制次数, 需在 1 小时内到达现场; 3. 每月出具运维报告, 报告应包含月度运维事件详细情况, 设备巡检记录截图、设备报警及安全隐患处理记录、设备资产变动清单、线路链接图变动清单、现存隐患及处置建议、设备版本及规则库更新情况、设备配置备份、设备配置变更详情截图; 4. 提供安全检测和分析平台, 针对服务提供数据 IP 资产 10 个, 云端加本地 7*24 小时持续不间断服务, 通过采集安全设备和工具的安全告警和安全日志, 结合大数据分析、人工智能等技术手	1	年	6%	99600	99600



		段，为用户提供安全威胁分析鉴定，同时在用户界面进行展示； 5. 提供 7*24 小时的安全守护，7*24H 在线服务； 6. ★支持通过云端平台查看安全事件详情查看攻击故事线，安全事件按照攻击入口和进程树的视角进行安全分析：（提供产品功能截图并加盖厂商公章） 7. 支持查看安全事件处置和响应建议，响应建议包括原理介绍、危害影响、处置建议：（提供产品功能截图并加盖厂商公章） 8. ★云端服务平台应当支持对接主要安全设备，支持实时接收安全设备检测到的安全事件信息、安全日志数据：（提供产品功能截图并加盖厂商公章） 9. 在服务范围内为发现的每一个高危可利用漏洞提供防护规则，承诺防护率达到 99%。					
总金额							2565000

甲方（盖章）：



日期：2025年3月7日

乙方（盖章）：



日期：2025年3月7日



附件 2:

网络与信息安全协议书

甲方应按照《中华人民共和国网络安全法》等法律法规的要求，履行相关网络安全义务，承担网络安全责任。

第一条 甲方承诺不利用乙方提供的服务及设备设施进行下列任何活动或发布、传播下列任何信息：

(1) 从事危害国家安全、泄露国家秘密等犯罪活动；从事国家法律、法规、政策所禁止的活动或违背公共道德的活动；

(2) 散布谣言，扰乱社会秩序，破坏社会稳定；散布垃圾邮件、病毒程序；黑客行为；侵权行为；博彩、赌博游戏等；

(3) 危害国家安全、泄露国家机密、颠覆国家政权、破坏国家统一的信息；损害国家荣誉和利益的信息；煽动民族仇恨、民族歧视、破坏民族团结的信息；违反国家宗教政策的信息；宣扬邪教和封建迷信的信息；淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的信息；侮辱或者诽谤他人，侵害他人合法权益的信息；妨碍互联网运行安全的信息；其他有损于社会秩序、社会治安、公共道德的信息或内容；

(4) 发布、传播其他违反国家法律、法规、政策内容的。

甲方同时承诺不为他人从事上述活动或发布、传播上述信息提供任何便利，如因甲方违反上述约定产生的一切责任和后果均由甲方承担。甲方认可乙方有权判断本协议项下甲方从事的活动或甲方发布的



信息是否违法、违规或违反本协议有关规定，且乙方有权在提前通知甲方的情况下采取一切必要措施，包括但不限于暂停或终止提供本协议项下的服务、要求甲方进行整改等，但乙方上述权利不应被视为乙方有审核甲方行为或信息内容的义务或保证其合法合规的任何责任。

第二条 甲方不得有下列危害电信网络和信息安全的行为：

(1) 对电信网络的功能或者存储、处理、传输的数据和应用程序进行违法删除或者修改。

(2) 利用电信网络从事窃取或者破坏他人信息、损害他人合法权益的活动。

(3) 故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施。

(4) 危害电信网络和信息安全的其他行为。

若甲方存在上述任一情形的，乙方有权按相关规定暂停或停止提供服务、断开网络接入，保存有关记录，并向政府主管部门报告，由此引起的一切后果和责任由甲方负责。同时，乙方有权终止合同，并不承担任何责任。

第三条 甲方不得将接入设备转借或租赁给其它单位和个人使用，以防止非法信息的传播；否则，由其承担相关责任，乙方有权立即停止相关服务。

第四条 甲方应承担如下管理责任：

(1) 向所属员工或使用者宣传国家及电信主管部门有关电信安全的法规规定。



(2) 建立健全使用者档案，加强对使用者的管理、教育工作。

(3) 有健全的网络安全保密管理办法。

第五条 甲方有责任对其自身系统的网络安全状况负责，并定期对其系统的安全状况进行检查，若发生网络攻击、信息泄露等网络安全事件，乙方不承担相关责任。

第六条 甲方侧数据由甲方负责，如出现信息泄露、信息篡改等安全事件，乙方不承担责任。

第七条 甲方承诺采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。不得从事以下行为：

(1) 利用自己或他人的机器设备，未经他人允许，通过非法手段取得他人机器设备的控制权；

(2) 非授权访问、窃取、篡改、滥用他人机器设备上的信息，对他人机器设备功能进行删除、修改或者增加；

(3) 向其他机器设备发送大量信息包，干扰其他机器设备的正常运行甚至无法工作；或引起网络流量大幅度增加，造成网络拥塞，而损害他人利益的行为；

(4) 资源被利用进行网络攻击的行为或由予机器设备被计算机病毒侵染而造成攻击等一切攻击行为

(5) 有意通过互联网络传播计算机病毒；

(6) 因感染计算机病毒进而影响网络和其它客户正常使用的行为。



第八条 甲方业务如使用乙方提供的 IP 地址,甲方需承诺并确认:甲方所提交的所有备案信息真实有效,且备案信息不得出现乙方任何内容。当提供的备案信息发生变化时应及时到备案系统中提交更新信息,如因未及时更新而导致备案信息不准确,乙方有权依法采取停止提供服务、断开网络接入等关闭处理措施。如因甲方原因造成信息未及时通知,引发相关网络信息安全事件的,由甲方自行承担相关责任。

甲方(盖章):



日期: 2025 年 5 月 7 日

乙方(盖章):



日期: 2025 年 5 月 7 日

河南移动 合同管理



河南移动 合同管理





附件 3:

移动云 IaaS 业务协议

根据《中华人民共和国民法典》、《中华人民共和国电信条例》等相关法律法规规定，本着平等自愿的原则，基于对乙方移动云业务的了解和需求，甲方同意购买和使用移动云业务，并与乙方达成本移动云业务协议：

一、服务内容

1.1 “移动云业务”是指基于中国移动云数据中心资源，乙方向用户提供的基础资源、平台能力、软件应用等服务。本协议项下甲方向乙方购买的移动云业务的具体类型及服务期限见附件一《移动云平台资源订购表》。

甲方向乙方订购附件一约定范围外的其他类型移动云业务的，可通过在线方式【<https://ecloud.10086.cn/>】办理。

1.2 乙方将依据本协议在约定的服务期限内向甲方提供移动云业务。

二、服务费用

2.1 本协议项下甲方向乙方购买的移动云业务的费用标准见附件一《移动云平台资源订购表》。

2.2 甲方向乙方订购附件一约定范围外的其他类型移动云业务的，乙方将根据甲方在移动云业务页面上实际订购的业务类型及情况，按照移动云业务页面上公示的【产品目录价（注：或产品目录价的*折）】向甲方收取服务费用。

2.3 服务费用以乙方根据甲方所购买服务的使用时间、流量、点击数等进行计费出账。服务费用账单由乙方计费系统出具，账单中应包含该计费账期内业务的实际发生情况、结算金额以及其它对账所需的业务信息。

2.4 计费账期



计费账期根据所选产品的收费周期核算，一般包含包年、包月、按量计费、一次性计费等方式，具体以移动云出账为准。

2.5 业务对账

甲乙双方约定，选择 ☒ 预付费 ☐ 后付费（__个月）的付费方式。



2.5.1 预付费：是指在甲方提前付费之后，乙方才开始为甲方提供服务。甲方应保证账户中预存的费用余额充足，以使得服务得以继续进行。

预付费余额不足而甲方需要继续使用服务的，甲方应当及时进行充值续费。如续费时移动云网站对移动云产品体系、名称或价格进行调整的，双方同意按照届时有有效的新的移动云产品体系、名称或价格执行。

除双方另有约定外，服务期满或本协议终止时，甲方已预付但未消费的款项，乙方将向甲方退还。乙方将根据双方最终实际结算金额向甲方开具税率为【6%】的增值税发票。

2.5.2 后付费：是指乙方先向甲方提供服务，并按约定的周期与甲方确认账单后，由甲方在约定的时间内向乙方支付服务费。具体执行如下：

(1) 业务对账：每计费账期结束后【10】个工作日内，乙方将该账期账单以【电子邮件】的方式发送给甲方。甲方应在收到该账期账单后【5】个工作日内，核对该账期的结算总金额并以【电子邮件】的方式与乙方确认账单。

(2) 结算付费：以【月度】为一个结算周期，甲方应在结算账单确认后【7】天内足额支付服务费。

(3) 若甲方对账单有异议的，双方应在【10】个工作日内重新对账并确定应结算金额。双方进行的重新对账不影响资金结算的正常进行。资金结算仍按照乙方出具的账单中所列金额进行结算，对账差异的调整在下一个结算周期内进行。对于最后一个结算周期出现的对账差异，双方多退少补。

(4) 乙方在收到甲方服务费后【10】个工作日内，按照该甲方支付金额向甲方开具税率为【6%】的增值税发票。

2.5.3 若双方对账出现误差，当误差金额不超过账单所列结算总金额的【3】%时，则双方按照乙方出具的账单所列结算总金额作为结算依据；当双方对账误差超过账单所列结算总金额的【3】%时，则双方应在【10】个工作日内重新对账并确定应结算金额。双方进行的重新对账不影响资金结算的正常进行。资金结算仍按照乙方出具的账单中所列金额进行结算，对账差异的调整在下一个结算周期内进行。对于最后一个结算周期出现的对账差异，双方多退少补。

2.6 服务费用并不包含甲方访问互联网或移动网络而产生的相关费用。

2.7 在甲方未按照约定支付全部费用之前，乙方保留不向甲方提供服务和/



或技术支持，或者终止服务和/或技术支持的权利。同时，乙方保留对欠费行为追究法律责任的权利。

2.8 乙方可能会定期或不定期开展优惠促销活动，活动方式包括但不限于打折或赠送服务，优惠促销期结束后，甲方在优惠促销期间所订购的资源产品将恢复正常价格计费。

三、甲方的权利、义务

3.1 甲方应严格遵守《中华人民共和国网络安全法》、《中华人民共和国电信条例》、《互联网信息服务管理办法》、《中华人民共和国反电信网络诈骗法》等有关法律法规规定，不得从事任何违法经营活动。

3.2 甲方同意接受和遵守移动云业务页面所公示的移动云业务规则、资费政策、服务承诺、SLA、法律声明、以及相关管理规范 and 流程（以下统称“业务规则”）。甲方了解上述业务规则的内容可能会不时更新。如上述业务规则的任何内容发生变动，乙方将通过提前【30】天在移动云业务页面的适当版面公告向甲方提示修改内容。如甲方不同意乙方对上述业务规则相关条款所做的修改，甲方有权停止使用移动云业务，在此情况下，乙方应与甲方进行服务费用结算（如有），并且甲方应将业务数据迁出。如甲方继续使用移动云业务，则视为甲方接受乙方对上述业务规则相关条款所做的修改。

3.3 甲方应按照本协议约定向乙方支付其所购买移动业务的各项服务费用。

3.4 甲方在登陆移动云业务时所使用的账户密码，包括注册账户密码以及乙方为方便业务办理根据甲方的申请以短信等方式向甲方提供的随机密码等服务密码，是甲方办理业务的重要凭证，甲方应注意保密并妥善保管。甲方应确保在每个上网时段结束时退出登录并以正确步骤离开移动云业务页面。如甲方发现账户密码遗失或被盗，甲方应及时进行修改或挂失。凡使用账户密码办理业务的行为（包括但不限于在线提交各类表单，订购、变更或终止业务，购买商品或服务以及发布信息）均被视为甲方或甲方授权的行为，甲方应承担因此产生的责任和义务。因甲方未妥善保管或不慎泄露账户密码导致的影响和损失，由甲方自行承担。

3.5 甲方在申请使用移动云业务时，必须向乙方提供真实、准确的注册信息，包括但不限于甲方的姓名/单位名称（及法定代表人/负责人姓名）、身份证件号



码/统一社会信用代码、住址/住所、联系人、联系方式、邮政编码、电子邮件地址等，以及注册资料，包括但不限于身份证件/营业执照（及税务登记证）等有效证件的复印件（单位证件应加盖公章）。如注册信息和注册资料有任何变动，应当及时更新，甲方未及时、准确、完整更新有关信息并通知乙方的，由此带来的任何损失及法律责任全部由甲方自行承担。

3.6 如甲方拒绝向乙方提供真实、准确的注册信息和注册资料，或者冒用他人证件，或者使用伪造、变造的证件的，乙方依法有权拒绝为甲方提供或继续提供移动云业务，由此带来的任何损失及法律责任全部由甲方自行承担。

3.7 甲方承诺：

3.7.1 甲方在使用业务用于互联网信息服务时，应按照监管部门要求全面落实网络信息安全管理举措并按乙方要求提供证明材料。如果甲方利用乙方提供的服务进行的活动需要获得国家有关部门的许可或批准的，应获得该有关的许可或批准。包括但不限于以下内容：如果甲方的网站提供非经营性互联网信息服务的，必须办理非经营性网站备案，并保证所提交的所有备案信息真实有效，在备案信息发生变化时及时在备案系统中提交更新信息；如甲方的网站提供经营性互联网信息服务的，甲方应自行向当地通信管理部门申请取得相应的增值电信业务经营许可证；如甲方经营互联网游戏网站的，甲方应依法获得网络文化经营许可证；如甲方经营互联网音、视频网站的，甲方应依法获得信息网络传播视听节目许可证；若甲方从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

甲方理解并认可，以上列举并不能穷尽甲方进行经营或非经营活动需要获得国家有关部门的许可或批准的全部类型，甲方应获得有关的许可或批准并应在服务期内持续有效，同时还应符合国家及地方不时颁布相关法律法规之要求。

3.7.2 除乙方明示许可外，甲方不得修改、翻译、改编、出租、转许可、在信息网络上传播或转让乙方提供的软件及产品，也不得反向工程、反编译或试图以其他方式发现乙方提供的软件及产品的源代码。

3.7.3 若移动云业务涉及第三方软件之许可使用的，甲方同意遵守相关的许可协议的约束。



3.7.4 不违法经营电信业务，不转租、转售乙方提供的电信业务。

3.7.5 不利用乙方提供的资源和服务上传、下载、储存、发布如下信息或者内容，不为他人发布该等信息提供任何便利：

- (1) 反对宪法所确定的基本原则的；
- (2) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (3) 损害国家荣誉和利益的；
- (4) 煽动民族仇恨、民族歧视、破坏民族团结的；
- (5) 破坏国家宗教政策，宣扬邪教和封建迷信的；
- (6) 散布谣言，扰乱社会秩序，破坏社会稳定的；
- (7) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- (8) 侮辱或者诽谤他人，侵害他人合法权利的；
- (9) 含有虚假、有害、胁迫、侵害他人隐私、骚扰、侵害、中伤、粗俗、猥亵、或其它道德上令人反感的内容；
- (10) 含有中国法律、法规、规章、条例以及任何具有法律效力之规范所限制或禁止的其它内容的。

3.7.6 不擅自向他人发送商业广告，不发送垃圾邮件、垃圾短信息等。

3.7.7 不进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP 欺骗、DOS 等）。

3.7.8 不运行影响乙方服务器正常工作的程序、进程，不进行任何改变或试图改变乙方提供的系统配置或破坏系统安全的行为。

3.7.9 不删除、修改或掩藏移动云业务相关软件及产品中包含的任何版权、商标或其他专有权声明。

3.7.10 不将移动云业务用于由于相关业务或产品故障而可能会导致死亡、严重人身伤害，或严重的物理或环境损害（以下简称“高风险使用”）的任何应用或情况。高风险使用的情况包括但不限于：飞机或其他大型交通工具、核设施或化工设施、生命支持系统、植入式医疗设备、机动车辆或武器系统；但是，高风险使用不包括，出于管理目的而利用产品来存储配置数据，利用工程和/或配置



工具或利用其他非控制性应用程序，以及在上述使用情形中即使出现故障，也不会导致死亡、人身伤害或严重的物质或环境损害的任何应用或情况。这些非控制性应用程序可能会与控制性应用程序进行通信，但不得直接或间接地对控制功能负责。

3.7.11 不利用乙方提供的服务从事损害乙方合法权益及第三方合法权益的行为。

3.7.12 不从事其他违法、违规或违反移动云业务条款的行为。

3.7.13 如乙方发现甲方违反上述条款的约定，有权根据情况采取相应的处理措施，包括但不限于立即中止服务、终止服务或删除相应信息等。另外，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，甲方有责任在规定时间内进行说明并出具证明材料，如甲方未能提供相反证据或甲方逾期未能反馈的，乙方将采取包括但不限于立即中止服务、终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。甲方同意，乙方对因采取上述措施产生的后果不承担责任。

3.8 甲方承诺不利用乙方提供的本合同项下服务从事任何下列情形之一的行为：涉案涉诈、IP 违规翻墙、资质与互联网网络接入资源使用用途不一致、超范围经营、层层转租、发布不良信息、参与“挖矿”活动、黑名单网站接入、未备案接入等违法违规问题。发现甲方使用乙方提供的本合同项下服务存在涉嫌上述情况的，乙方有权根据情况采取相应的处理措施，包括但不限于立即中止服务、终止服务或删除相应信息等。

3.9 甲乙双方同意，上述 3.5-3.8 约定的情形从根本上违背本合同目的。乙方有权采取包括但不限于各种技术手段在内的措施检测识别、排查处置甲方使用乙方提供的本合同项下服务的行为，发现涉嫌上述情形的，乙方有权根据危害程度，决定单方解除本合同，由此产生的责任与后果由甲方承担。

3.10 甲方有责任对自身信息系统的安全状况负责，并定期对自身信息系统进行安全状况检查。甲方不应在移动云平台之上安装、使用盗版软件；甲方对自己行为（如自行安装的软件和进行的操作）所引起的结果承担全部责任。甲方应积极配合国家相关部门和乙方对网络安全事件的跟踪、调查，并提供相关的信息和资料。



3.11 甲方应向乙方提交执行本协议的联系人和管理用户网络及云平台上各类产品与服务的人员名单和联系方式并提供必要的协助。如以上人员发生变动,甲方应自行将变动后的信息进行在线更新并及时通知乙方。因甲方提供的人员的信息不真实、不准确、不完整,以及因以上人员的行为或不作为而产生的结果,均由甲方负责。

3.12 甲方了解乙方无法保证其所提供的服务毫无瑕疵,但乙方承诺不断提升服务质量及服务水平。所以甲方同意:即使乙方提供的服务存在瑕疵,但上述瑕疵是当前行业技术水平所无法避免的,其将不被视为乙方违约。甲方同意和乙方一同合作解决上述瑕疵问题。

3.13 乙方将负责操作系统以下的底层部分及甲方提供软件的运营维护。操作系统及操作系统之上部分(如在系统上安装的应用程序等)由甲方自行负责。如果甲方订购的云主机等产品出现死机等情况,甲方可通过平台自行重启系统,也可以授权乙方帮助进行系统重启,但乙方不对重启后的结果承担任何责任。

3.14 数据备份是甲方的义务和责任。虽然乙方可能会配置具有日常数据备份功能的工具,但并不意味着数据备份是乙方的义务。乙方不保证完全备份用户数据,亦不对用户数据备份工作或结果承担任何责任。

3.15 移动云服务平台上可能存在由第三方提供的产品或服务,乙方无法对第三方产品或服务的质量向甲方提供保证。甲方在使用第三方产品或服务前,应在仔细阅读相关产品或服务的使用说明及相关协议后决定是否使用。因使用第三方产品或服务产生的纠纷,由甲方直接与第三方协商解决。

3.16 甲方有义务协助乙方完成业务开通的验收确认,并根据相关业务要求签订业务验收或交付报告。甲方经乙方通知验收后怠于履行验收义务,未签订业务验收或交付报告的,视为甲方验收合格,甲方后续不得主张乙方交付的业务不符合合同约定。



四、乙方的权利、义务

4.1 乙方应按照本协议约定提供服务、收取服务费用。

4.2 服务期限内,乙方将为甲方提供如下客户服务:

4.2.1 乙方为甲方提供 7×24 售后服务,并为甲方提供有效的联系方式并保证



甲方能够进行故障申报。

4.2.2 乙方将消除甲方非人为操作所出现的故障，但因甲方的原因和/或不可抗力以及非乙方控制范围之内的事项除外。

4.3 乙方将按照移动云业务页面上所公示的《服务等级协议》（SLA），确保移动云平台的服务可用性和数据可靠性。

4.4 乙方会依法履行保密义务。

4.5 为向甲方提供更好的服务，方便甲方了解乙方的各类业务、各类营销优惠活动及相关信息，甲方同意乙方可以以短信、彩信、电话、电子邮件、信函等方式就业务和服务与甲方进行沟通，包括但不限于向甲方发出产品和服务信息。

4.6 基于电信技术的发展，按照相关法律法规、政府指令、行业规划或业务调整的需要，乙方可以停止提供本协议项下的服务（包括但不限于网络服务、用户服务、电信服务及其他相关服务），但应提前向甲方发送通知。如遇紧急突发情况，乙方可以立即停止提供本协议项下的服务，但应尽量提前向甲方发送通知。甲方同意，乙方对因采取上述措施产生的后果不承担责任。

五、用户信息和数据

5.1 为了保障甲方使用本协议项下服务的安全以及不断改进移动云业务质量，移动云业务系统将记录并保存甲方登录和使用本协议项下服务的相关信息。

5.2 甲方的用户信息和数据将在下述情况下部分或全部被披露：

5.2.1 经甲方同意，向第三方披露；

5.2.2 根据法律法规的有关规定，或者行政、司法机关的要求，向第三方或者行政、司法机关披露；

5.2.3 如果甲方出现违反中国有关法律法规的情况，需要向第三方披露；

5.2.4 为提供甲方所要求的软件或服务，而必须和第三方分享甲方的用户信息和数据。

5.3 乙方仅得按当前行业技术水平提供相应的安全措施以使移动云业务系统存储的用户信息和数据不丢失，不被滥用和篡改，这些安全措施包括向其他服务器备份数据和对用户密码加密。鉴于计算机及互联网的特殊性以及网络安全技术的局限性，甲方理解，尽管有这些安全措施，但移动云仍然不能保证甲方的用户信息和数据的绝对安全。



5.4 对于甲方通过移动云业务上传、下载、储存、发布的内容，乙方有权根据国家相关法律法规和网络信息安全管理的规定，以及本协议其他约定，进行必要的监督和审查。

5.5 甲方理解并同意：在向甲方提供移动云业务的过程中，基于运维管理等需要，乙方有可能对甲方在移动云系统中存储的数据进行迁移、维护等操作，上述数据迁移、维护操作是乙方为向用户提供移动云业务所必须的，不构成对甲方的隐私资料、保密信息的任何侵犯。甲方同意并授权乙方（在履行保密义务并采取适当保护措施的情况下）可以进行上述数据迁移、维护操作。甲方保证其上述授权行为已经获得了所有必要的同意、许可并遵从了所有可适用的法律法规的要求。

5.6 除法定及甲乙双方另行约定外，自本协议约定的服务期满或因任何原因导致本协议提前终止的，乙方将自终止之日起继续存储甲方的数据 10 个自然日，逾期将不再保留甲方的数据，甲方应在上述期限届满前自行做好数据备份工作，因未及时备份数据所产生的一切后果由甲方自行承担。

六、知识产权

6.1 甲方应保证提交给乙方的素材、对乙方服务的使用及使用移动云业务所产生的成果未侵犯任何第三方的合法权益。如有第三方基于侵犯版权、侵犯第三人权益或违反中国法律法规或其他适用的法律等原因而向乙方提起索赔、诉讼或可能向其提起诉讼，则甲方应赔偿乙方因此承担的费用或损失，并使乙方完全免责。

6.2 如果第三方机构或个人对甲方使用移动云业务所涉及的相关素材的知识产权归属提出质疑或投诉，甲方有责任出具相关知识产权证明材料，并配合乙方相关投诉处理工作。

6.3 甲方承认乙方向甲方提供的任何资料、技术或技术支持、软件、服务等知识产权均属于乙方或第三方所有。除乙方或第三方明示同意外，甲方无权复制、传播、转让、许可或提供他人使用上述资源，否则应承担相应的法律责任。

七、保密条款



7.1 “保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接收方”）提供的信息，或接收方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于：技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接收方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方书面同意，接收方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。但是，乙方为本协议目的向其经营电信业务的关联方披露保密信息不受本条约束。

7.3 本协议双方同意尽最大的努力保护上述保密信息等不被披露。一旦发现上述保密信息泄露事件，双方应合作采取一切合理措施避免或者减轻损害后果的产生。

7.4 本保密条款不因本协议的终止而失效。

八、违约责任

8.1 如甲方未按约定支付服务费用，乙方有权暂停为甲方提供本协议项下的服务，并按照《中华人民共和国电信条例》第三十四条规定，自甲方欠费之日起至甲方付清欠费之日止每日按全部欠费金额的3‰向甲方加收违约金。甲方在暂停服务后60日内仍未补交服务费用和违约金的，乙方有权终止向甲方提供本协议项下的服务，并有权继续追索甲方所欠的全部费用及其违约金，由此带来的任何损失及法律责任全部由甲方自行承担。

8.2 因甲方违反法律法规或本协议约定，乙方依法或依据本协议约定终止向甲方提供本协议项下服务的，乙方有权不退还甲方已经支付的费用，并有权释放甲方所订购服务占用的资源，由此带来的数据丢失等损失全部由甲方自行承担。

8.3 如乙方向甲方提供的移动云业务不符合本协议约定，乙方将尽商业上合理的努力修正错误，服务可用性等级指标及赔偿方案按照届时有效的《服务等级协议》（SLA）执行。如果乙方无法以商业上合理的方式实质性修正错误导致甲方无法继续正常使用移动云业务，甲方有权终止使用移动云业务，并获得与尚未



使用服务部分相对应的退款。

8.4 乙方仅对因其过错给甲方造成的直接损害结果依法承担赔偿责任，在任何情况下，乙方均不对任何间接性、后果性、惩戒性、偶然性、特殊性的损害，包括甲方使用移动云业务而遭受的利润损失、记录或数据的丢失或损坏承担责任。除法律法规另有强制性规定外，在任何情况下，乙方对本协议项下所承担的违约金及赔偿总额之和不超过甲方向乙方实际支付费用的总和。

8.5 除本协议另有约定外，甲方理解并同意，下述情况不属于乙方违约：

(1) 乙方在进行数据中心机房整顿、扩容、变更服务器托管地点、服务器配置、维护、数据迁移等操作时，需要短时间中断服务；

(2) 因不可抗力或意外事件，使得本协议的履行不可能、不必要或者无意义的。不可抗力、意外事件是指不能预见、不能克服并不能避免且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如暴雨、洪水、海啸、风暴、地震、火山喷发、泥石流、火灾、干旱、雷电、疫病流行等以及社会事件如战争、动乱、恐怖袭击、罢工、法律政策变化、政府行为、通信网络中断或阻塞、移动网关出错、黑客攻击等网络安全事故、网路堵塞、电信部门技术调整和通信管制等。

九、法律适用和争议解决

9.1 本协议的成立、效力、解释、履行、变更、终止以及争议的解决均应适用中华人民共和国法律。

9.2 对本协议未尽事宜，由双方协商解决。如双方协商不成的，任何一方均有权向乙方住所地人民法院提起诉讼。

十、其他

10.1 本协议自甲乙双方加盖单位印章之日起生效，如双方签署时间不一致，自较迟的签署日起生效。本协议将保持其效力直至附件一约定的服务期限届满且双方已完全履行协议项下的所有义务且双方之间的所有付款和索赔已结清。

10.2 甲方在移动云业务页面上订购附件一约定范围外的其他类型移动云业务的，或者协议签署后资源开通期间，出现移动云官网资费变动、产品规格变动



等情况，可以以甲方在业务办理过程中提交的并经乙方受理确认的业务申请单/订购单（甲方确认同意的订购页面）等各类表单、业务协议等进行补充，以上凭据均构成本协议不可分割的组成部分，与本协议具有同等法律效力。

10.3 乙方在移动云业务页面上所公示的业务规则构成本协议不可分割的组成部分，与本协议具有同等法律效力。

附件一：《移动云平台资源订购表》



河南移动 合同管理



河南移动 合同管理



附件一：平台资源订购表

平台资源订购表											
产品名称 大类	产品名称 小类	规格 型号	操作系 统类型	目录 单价 (元)	计费 模式/ 计费 标准	数 量	折 扣	合 同 期 限 (月)	合 同 价 (元 /月)	合 同 价 (元 /年)	备 注
云主 机	通用 型云 主机	s5. x1 arge. 2	Window s	4572	包年	1	50%	12	190. 5	2286	
系统 盘	性能 优化 型	50GB	/	210	包年	1	50%	12	8.75	105	
数据 盘	性能 优化 型	150GB		630	包年	1	50%	12	26.2 5	315	
IPv4 带宽	按带 宽计 费	5Mbps	/	1200	包年	1	50%	12	50	600	
合计										3306	



(合同签署页)

合同名称：【移动云业务协议】

甲方：【漯河市源汇区卫生健康委员会】 (盖章)

法定代表人或授权代表：

日期：

2025.3.7

乙方：【中国移动通信集团河南有限公司漯河分公司】 (盖章)

法定代表人或授权代表：

日期：

2025.3.7