甲方合同编号：【　　】

乙方合同编号：【　　】

开封市卫生健康委员会卫生专网升级改造服务项目

技术服务合同

甲方：【开封市卫生健康委员会】（盖章）

法定代表人/负责人：【郑红英】

住所：【开封市金明大道157号】

法定代表人/授权代表签字：

联系人：【杨洋】

电话：【15093694081】

乙方：【中移建设有限公司】（盖章）

法定代表人/负责人：【孙卫东】

住所：【北京市海淀区北蜂窝路18号（综合楼9层906、907、917）】

授权代表签字：

联系人：【赵鸿越】

电话：【15037828560】

协议签订地：【开封市】

合同签订日期：【2026】年【8】月【6】日

鉴于本合同为甲方委托乙方就【开封市卫生健康委员会卫生专网升级改造服务】项目进行的专项技术服务，并支付相应的技术服务报酬。为明确各自的权利和义务，双方经过平等协商，根据《中华人民共和国民法典》等有关法律法规的规定，订立本合同。

第一条、技术服务项目概要

1.1 技术服务的内容：【开封市卫生健康委员会卫生专网升级改造服务】

1.2 技术服务的方式：【提供现场指导和服务】

1.3 技术服务地点：【甲方指定服务地点】

1.4 技术服务期限：【3 年服务期】

1.4.1 乙方承诺：本项目约定的 3 年技术服务期限届满后，乙方额外向甲方免费提供 2 年与原合同服务内容及标准相同的技术服务（自原技术服务期限届满次日起算），赠送服务期内乙方服务标准不得低于本合同约定的服务标准。

1.5 乙方为甲方提供的具体服务相关具体要求详见附件【技术规范书】。

1.5.1 甲方有权在合同履行期间对乙方的服务质量、服务进度和服务人员进行监督与检查，乙方应予以配合。甲方发现乙方服务存在问题的，有权要求乙方限期整改，乙方应在甲方要求的期限内完成整改。

第二条、技术服务报酬和支付方式

2.1 本合同项下甲方应当向乙方支付的服务费用共计【1455000】元（大写：人民币壹佰肆拾伍万伍仟元整），增值税税率为【6%】。当合同约定的税率与国家税法规定及税务机关认定的税率不一致时，以国家税法规定及税务机关认定的税率为准进行调整，调整时以本条款不含税价为基准，执行国家法规及规范规定及税务机关规定的税率。任何有关合同价格的修改，都必须用纸质书面形式，由双方共同签订后方可生效。

2.2 合同项下所有款项由甲方向乙方以如下方式及比例支付：

本项目款甲方分两次付款给乙方，2026 年 12 月份前甲方支付本合同款总金额的 50%，即（人民币大写：柒拾贰万柒仟伍佰元整，小写：¥727500）给乙方。2027 年 12 月份前甲方支付本项目剩余 50%项目款给乙方，即（人民币大写：柒拾贰万柒仟伍佰元整，小写：¥727500）。

上述付款进度为甲方向财政部门申请支付的时间安排，具体支付以财政拨款实际到账时间为准。因财政支付进度导致延迟的，不属于甲方违约，甲方不承担逾期付款的违约责任。甲方在收到乙方合规发票及付款申请后应及时启动财政支付申报程序，并以书面方式将财政支付进度告知乙方。

2.3 甲方向乙方结算相关信息如下：

甲方名称：【开封市卫生健康委员会】

纳税人识别号：【11410200005316960 8】

户名：【开封市卫生健康委员会】

开户行：【中行开封集英街分行】

账号：【248144671551】

地址：【开封市金明大道 157 号】

邮政编码【XXX】

电话【15093694081】

电子邮件【XXX】

乙方名称：【 中移建设有限公司 】

纳税人识别号：【 911101087481059966 】

户名：【中移建设有限公司】

收款开户行：【 招商银行股份有限公司北京分行营业部 】

收款帐号：【 8888014900013144 】

开票账号：【11050190360009000777】

开票开户行：【中国建设银行北京月坛支行】

地址：【 北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917） 】

邮政编码【450000】

电话【15037828560】

电子邮件【/】

2.4 结算方式采用【转账】的形式。

2.5 在甲方支付本合同项下的服务费之前，乙方应当向甲方开具相应金额的增值税【普通】发票。

第三条、组织与管理

3.1 甲方提供项目需求的工作条件以及实施地点；

3.2 在本合同有效期内，乙方委派技术人员为甲方提供技术服务。

3.3 本合同甲、乙双方分别指定项目负责人如下：

（1）甲方负责人：【杨洋】，电话：【15093694081】

（2）乙方负责人：【赵鸿越】，电话：【15037828560】

3.4 项目负责人的主要职责为：

（1）牵头组织本方技术服务工作；

（2）负责组织协调合同的签订、履行；

（3）负责跟踪或报告技术服务工作进展和成果；

（4）负责与另一方的沟通协调、信息传递等工作，为技术服务工作提供便利条件。

3.5 协议各方变更项目负责人的，应当及时以书面形式通知另一方。

第四条 验收

4.1 验收标准：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 双方应对项目服务质量，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。甲方自收到乙方提交的完整验收申请及全部交付物后【15】个工作日内组织验收。如验收不合格，乙方应在【10】个工作日内完成整改并重新提交验收申请，由此产生的费用由乙方承担。甲方自收到乙方提交的完整验收申请后【15】个工作日内未组织验收，且自乙方书面催告后【7】个工作日内仍未组织验收且无正当理由的，视为验收通过。

第五条 双方的权利与义务

5.1 甲方的权利和义务

5.1.1 在本合同有效期内，甲方有权要求乙方根据本合同约定向甲方提供相应的服务。

5.1.2 乙方可委托第三方从事部分合同约定的服务工作，但须事先书面告知甲方并取得甲方书面同意。乙方应对第三方的服务行为向甲方承担责任。

5.1.3 甲方应当根据其项目实施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）。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，使乙方无法将服务提供给甲方，甲方承担由此造成的责任和后果。

5.1.4 甲方承诺并保证不利用乙方提供的集成维保服务进行任何违反国家政策、法

律法规以及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。

5.1.5 甲方应本合同的约定，及时足额向乙方支付各项费用。

5.1.6 甲方开通使用乙方提供的相关产品时，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的，相关责任由甲方承担。

5.1.7 未经乙方同意，甲方不得将乙方的专有软件、专有技术、设施等用于双方合作项目以外的其他用途，且不得向第三方泄露或非法转让。若甲方违反本条款，乙方有权要求甲方赔偿因此给乙方造成的直接损失，终止协议。（甲方为履行政府公共职能或根据法律法规、上级主管部门要求使用相关成果的，不受上述限制。）

5.1.8 甲方有权在合同履行期间对乙方的服务质量、服务进度和服务人员进行监督与检查，乙方应予以配合。甲方发现乙方服务存在问题的，有权要求乙方限期整改，乙方应在甲方要求的期限内完成整改。

5.2 乙方的权利和义务

5.2.1 乙方从事系统集成、维护等工作，需由乙方人员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。

5.2.2 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服务的，应提前通知甲方，甲方应给予必要的配合。

5.2.3 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。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。

5.2.4 因甲方设备问题导致乙方无法正常提供本合同约定服务的，由甲方承担相应

责任。

5.2.5 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。

5.2.6 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。

第六条、知识产权

6.1 本合同由甲方提供的软件、资料和其他产品，所有权归甲方。

6.2 在本合同有效期内，甲方利用乙方提交的技术服务工作成果所完成的新的技术成果，归甲方所有。

6.3 在本合同有效期内，乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，包括但不限于软件、算法、技术方案等，其知识产权归甲方所有。乙方在履行本合同过程中使用的既有的知识产权仍归乙方所有，但甲方享有在本项目范围内永久免费使用的权利。

6.4 本合同对于在服务实施期间，一方独立或双方联合开发或提供的与本服务主题相关的概念或技巧，本合同对双方的使用不加限制，但不得侵犯适用的专利和著作权。

第七条、保密条款

7.1 双方不得向任何人透露客户单位的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除客户单位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。

7.2 甲、乙双方的律师、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，双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。

7.3 如相关政府部门或监管机构要求本协议各方中的一方披露任何保密信息，该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。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）在保密信息提供方依据本协议做出披露前，保密信息接受方已合法拥有的信息；（3）保密信息接受方从有权披露的第三方获得的信息；及（4）保密信息接受方独立开发的信息，未使用任何保密信息。

7.4 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。

第八条 违约责任

8.1 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。

8.2 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。

8.3 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和赔偿责任：

（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、法规和政策的活动；

（3）甲方利用乙方提供的产品和服务从事其他不当用途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。

8.4 乙方仅对因其故意或重大过失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合同总金额的总和。但因乙方违反知识产权约定、保密义务或网络安全义务给甲方造成的损失，不受前述赔偿总额上限的限制。

8.5 甲方逾期支付服务费用的（因财政支付进度导致延迟的除外），每逾期一日按逾期金额的万分之五向乙方支付违约金，但违约金总额不超过逾期金额的 5%。

第九条 合同变更和解除

9.1 甲、乙双方经协商一致可变更或解除合同，应当以书面形式确定。

9.2 因对方违约致使合同不能实现合同目的或者已经无法继续履行的，合同一方可以向另一方提出变更或者解除合同的书面请求，另一方应当在 10 日内予以书面答复；逾期未于书面答复的视为不同意。

9.3 法律规定的合同解除情形出现时，一方主张解除合同的，应当书面通知对方。合同自通知到达对方时解除。

第十条 不可抗力及免责条款

10.1 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。

10.2 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延迟履行或部分履行本合同的原因说明。

10.3 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。

10.4 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。

10.5 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。上述情形下，乙方应及时通知甲方并出具相关合理证明材料，并应尽合理努力在 24 小时内恢复服务，及时向甲方报告处理进度。

第十一条 通知与送达

11.1 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。

11.2 上述书面通知按对方在本合同结算信息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，因迟延通知而造成的损失，由延迟通知方承担责任。

11.3 双方将按如下约定确定通知送达完成时间：

11.3.1 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；

11.3.2 以特快专递形式发出的通知，必须向本合同结算信息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。

第十二条　争议解决

12.1 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。

12.2 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，则双方同意向甲方住所地人民法院提起诉讼。

12.3 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。

第十三条 其他约定

13.1 本合同自甲、乙双方授权代表签字并加盖公章或者合同专用章之日起生效。本合同一式【肆】份，双方各持【贰】份，具有同等法律效力。

13.2 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。

13.3 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。

13.4 在本协议有效期内，双方可以通过友好协商，可以对本协议相应条款以协议方式变更或者解除本协议。有下列情形之一的，甲方有权单方解除本合同，并要求乙方退还已支付的全部费用，赔偿甲方损失：（1）乙方提供的服务质量严重不符合本合同约定，经甲方书面通知后在 30 日内仍未纠正的；（2）乙方将本合同服务全部转包给第三方的。除本合同另有约定外，单方面解除协议的一方，应对另一方因此遭受的直接损失承担全部赔偿责任。

第十四条 本合同附件

附件 1：技术规范书

附件 2：网络与信息安全承诺书（以下无正文）

附件 1：技术规范书

服务范围：

序号	内容名称	数量	单位
1	卫生专网升级改造三医网融合服务	3500	个
2	网络工具巡检服务	3	年
3	入侵检测与防御安全服务	3	年
4	安全审计服务	3	年
5	网络边界病毒过滤与恶意代码防护服务	3	年
6	政务远程加密接入安全服务	3	年
7	核心网络物理隔离服务	3	年
8	漏洞扫描服务	3	年
9	重保值守网络故障应急响应服务	3	年
10	安全运营分析与网络资产梳理服务	3	年
11	网络节点变更支持	3	年
12	应急演练	3	年

优惠承诺：本项目三年技术服务到期后，我公司将额外赠送 2 年技术服务。赠送服务期内服务标准不得低于本合同约定的服务标准。

分项服务详细技术要求

1、开封市卫生健康委员会卫生专网割接融合（三医一张网）服务要求

提供切实可行的割接方案，保障业务连续性、功能满足兼容与对等、性能满足业务负载。在不影响现有业务正常运行的前提下，将相关医疗业务流量合规迁移至电子政务外网，实现两网安全可控、高效稳定的互联互通。本次对接覆盖医保、医疗、公卫、药监等多类业务系统，不同业务在技术特性、接入要求及现有网络部署等方面存在差异，需制定针对性适配方案，统筹兼顾业务现状、用户使用体验与安全管控要求。

服务类型	技术类型	内容及要求
卫生专网割接融合（三医一张网）服务要求	服务内容	1.割接融合覆盖范围：涉及二级以上公立医院 31 家，二级以上民营医院 14 家，社区卫生服务中心、乡镇卫生院 108 家，疾病预防控制中心 11 家，2439 家村卫生室。 2.原有平台对接与部署:充分了解现有平台网络结构和业务系统情况，更新现有平台老旧网络工具（核心路由器 1 台、核心交换机 2 台）、优化网络拓扑，电子政务外网与卫生专网的 IP 地址规划，应在遵循行业标准和技术规范的前提下，贯彻分层规划、有序隔离、灵活扩展的基本原则，保障地址资源使用合理、高效、具备可扩展性。具体技术要求如下： 2.1.要求由 10 地址或 172 地址直接转换为 59 地址,不采用多次地址转换模式。 2.2.两网接入区的 59 地址建议规划分配至卫生专网侧,若存在特殊情况,各单位可根据实际需求灵活调整。

		2.3.两网内部均应采用私用 IP 地址段开展分层规划，同一城市内两网的地址空间必须严格隔离，不得存在任何重叠或冲突。 2.4.地址规划需采用分层化、结构化的设计思路，依照业务类型、区域、接入层级进行分层划分，为后续路由汇总、流量隔离、运维定位提供基础支撑。 2.5.接口互联地址、业务段地址、设备管理地址需分别采用独立地址段进行规划，禁止不同用途的地址段混用。 2.6.医疗机构现有内部网络地址原则上保持不变。市级部门负责统一规划安全接入区的外联地址池及 NAT 映射规则，以此减少对基层接入单位的扰动。 提升网络传输稳定性与规范性需兼容现有卫生信息系统架构及原有全省卫生专网骨干网网络，确保与省、市两级卫生信息平台无缝对接，并提供全周期技术支撑与调测验证服务。 3.医保专网： 医保结算业务为医疗行业核心基础业务，对实时性、稳定性、安全性要求极高，本次适配采用“保持现状、逻辑隔离、分层互通”方案，最大限度降低对现有医保业务运行的影响。 4.卫生专网业务： 卫生专网业务流量为本次对接的主要承载对象，采用

		“分层接入、统一转发、逻辑隔离”的适配方案，保障业务流量高效转发。 疾控业务： 疾控平台对接入的规范性、可溯源性、安全性有特殊技术要求，需采用“统一映射、合规转发、严格审计”的适配方案，在符合疾控平台技术标准要求的前提下，可实现业务交互。 5. 应急处置及应急回退预案： 做好应急处置预案及业务回退预案，做到融合割接万无一失。在对接实施过程中，若出现业务异常或安全事件，需立即按照应急处置预案开展处置工作，保障业务不中断。若割接过程中出现异常且无法在短时间内排查修复，需立即启动回退预案流程，将业务流量恢复至原有网络，保障业务正常稳定运行，然后排查问题原因，原因排查后再次进行业务割接。 业务中断平均恢复时长要求（单位：小时） I 级：≤0.5 小时 II 级：≤1 小时 III 级：≤1.5 小时 III+级：≤4 小时 IV 级：≤4 小时 普通级：≤4 小时 一般故障：≤24 小时

		紧急故障，30 分钟内响应，涉及硬件、光缆故障 4 小时内完成处理
人员要求	服务人员	服务方需了解开封市电子政务外网、开封市卫生健康委会员卫生专网、开封市医保网、开封市药监网现有网络架构，并具有电子政务外网网络实施部署经验。
服务频率	单次交付	
服务交付物	《卫生专网骨干网与电子政务外网双网融合交付报告》	

2、网络工具巡检服务

服务类	技术类型	内容及要求
网络工具巡检服务	服务内容	对开封市卫生健康委员会卫生专网工具运行状态的定期检查和分析能够及时把握网络运行情况，发现网络运行中的隐患问题，减小或规避安全事件的发生，减小网络故障对日常使用的影响。
服务频率	每月一次	
服务交付物	《网络工具巡检服务报告》	

3、入侵检测与防御安全服务

服务类型	技术类型	内容及要求
入侵检测与防御安全服务	服务内容	1.对跨网业务流量进行深度检测，实时识别并阻断针对医疗业务系统的攻击行为、恶意代码传输、异常漏洞利用等网络攻击流量，保障业务层安全。确保所有跨网业务流量都经过工具检测。工具的转发性能需匹配接入链

		路的带宽峰值。采用双机冗余模式部署 2.作为两网边界的核心安全防护工具，执行基础的访问控制策略，基于五元组实现流量的允许与拒绝。同时完成双向地址转换及端口映射功能，屏蔽两网的内部网络细节，采用双机冗余模式部署，确保工具级高可用性。上连电子政务外网核心节点，下连卫生专网核心节点，采用三层路由接口配置。
工具要求	服务工具	1.满足骨干接入安全防护要求，同时能够承载全市医疗机构接入要求。 2.支持多种部署模式，支持透明、路由、网线、混合等多种模式。 3.具有符合行业标准的规则库，防御特征库、漏洞特征库、病毒特征库、Web 应用防护规则库。 4.能够对访问业务资源的流量进行深度检测与阻断，重点防护医疗业务系统、数据库的通用漏洞攻击、恶意代码传输、异常流量、SQL 注入、跨站脚本攻击等常见攻击行为。 5. 配置日志服务器地址，将所有检测日志、攻击日志上传至日志审计系统，特征库自动更新，定期更新特征库版本。 6.满足骨干接入安全防护要求，同时能够承载全市医疗机构接入要求。

		7.满足 NAT 转换要求以及路由协议部署要求。 8.具有 IPv4/IPv6 一体化安全防护能力：符合细粒度访问控制能力，可基于源地址、目标地址、协议端口、应用层特征必须与业务需求严格匹配。 9.具有安全防护能力，能够在一体化访问控制策略中启用入侵防御、病毒防护、应用层过滤、DDOS 等安全能力。 10.能够基于黑白名单模式，可设置严谨的业务访问能力，可设置国家、地理位置等访问规则。 11.配置日志服务器地址，将所有检测日志、攻击日志上传至日志审计系统。特征库自动更新，定期更新特征库版本。
服务频率	每月一次	
服务交付物	《入侵检测与防御安全服务报告》	

4、安全审计服务

服务类型	技术类型	内容及要求
安全审计服务	服务内容	对所有跨网访问行为、流量转发状态及安全设备操作日志、NAT 日志进行全量记录，覆盖网络层、业务层、应用层的所有交互行为。日志留存时间需满足行业监管要求，最低留存期限为 180 天。
工具要求	服务工具	采用旁路部署模式，通过交换机镜像口获取所有跨网流量日志。同时采集防火墙、IPS/IDS 等安全设备的运行日志，具备单独的日志存储资源。
服务频率	每月一次	
服务交付物	《安全审计服务报告》	

5、网络边界病毒过滤与恶意代码防护服务

服务类型	技术类型	内容及要求
网络边界病毒过滤与恶意代码防护服务	服务内容	对跨网传输的文件、数据进行病毒特征查杀，实时过滤恶意病毒、木马等恶意代码，避免恶意代码通过跨网交互在两网内部扩散传播，保障终端与业务系统的安全。需支持病毒特征库在线自动更新，确保可识别最新的恶意代码样本。所有跨网传输的文件流量都需经过防病毒网关检测查杀，防病毒网关转发性能需匹配接入链路带宽峰值，针对需要跨网交互的大文件业务场景，需单独预留足够的性能冗余，避免影响业务传输效率。采用双

		机冗余模式部署。
工具要求	服务工具	1.满足骨干接入安全防护要求，同时能够承载全市医疗机构接入要求。 2.支持多种部署模式，支持透明、路由、网线、混合等多种模式。 3.具有符合行业标准的病毒库，能够对交互文件的流量进行深度检测与分析，实时过滤恶意病毒、木马等恶意代码，避免恶意代码通过交互过程中扩散传播。 4.配置日志服务器地址，将所有检测日志、攻击日志上传至日志审计系统。病毒库自动更新，定期更新特征库版本。
服务频率	每月一次	
服务交付物	《网络边界病毒过滤与恶意代码防护服务报告》	

6、政务远程加密接入安全服务

服务类型	技术类型	内容及要求
政务远程加密接入安全服务	服务内容	通过建立互联网加密传输通道，满足我市 3000+家村卫生室的互联网接入和业务访问需求。

工具要求	服务工具	1.涉及村卫生室业务访问要求，采用数据加密传输模式，通过搭建虚拟 VPN 网关接入。 2.满足 3000 用户并发访问要求。 3.配置日志服务器地址，将所有检测日志、攻击日志上传至日志审计系统。
服务频率	每月一次	
服务交付物	《政务远程加密接入安全服务报告》	

7、核心网络物理隔离服务

服务类型	技术类型	内容及要求
核心网络物理隔离服务	服务内容	通过物理隔离+数据摆渡的方式实现两网更高安全等级的隔离交换，对数据安全有极高要求、严格阻断底层网络连通性的场景。在核心业务系统与外部网络边界位置，通过专用硬件架构切断网络之间的链路层连接，仅支持按需进行合规数据交换，严格阻断外部网络对内部核心医疗业务系统的直接访问通路，从物理层面阻断跨网攻击渗透路径，保障核心敏感医疗数据的安全。
工具要求	服务工具	通过安全隔离工具实现网络隔离，严格控制，按需进行合规数据交换，严格阻断外部网络对内部核心医疗业务系统的直接访问通路，保障核心敏感医疗数据的安全。
服务频率	每月一次	
服务交付物	《核心网络物理隔离服务报告》	

8、漏洞扫描服务

服务类型	技术类型	内容及要求
漏洞扫描服务	服务内容	漏洞扫描是对我市“三医一张网”系统信息安全保障工作的基础和重要环节，发现主机、业务系统、中间件等安全漏洞，客观评估网络风险等级。根据检测结果给出对应安全修复加固建议，防范黑客攻击。
工具要求	服务工具	1.定期对所有网络设备、安全设备、业务系统开展漏洞扫描，及时发现并修复漏洞。 2.配置日志服务器地址，将所有检测日志、攻击日志上传至日志审计系统。漏洞库自动更新，定期更新特征库版本。
服务频率	每季度一次	
服务交付物	《漏洞扫描报告》	

9、重保值守网络故障应急响应服务

服务类型	技术类型	内容及要求
重保值守网络故障应急响应服务	服务内容	1.重保服务主要为“三医一张网”核心系统重大活动期间提供的特殊保障服务或配合上级安全检查工作，保障重要活动节假日召开期间网络安全可靠运行，全面提高安全运维队伍应对突发情况的综合管理水平和应急处置能力，最大限度地保证网络安全稳定运行和可靠畅通。 2.当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助用户快速止损，

		最大化降低安全事件带来的影响。
服务频率	即时响应	
服务交付物	《重保值守网络故障应急响应服务报告》	

10、安全运营分析与网络资产梳理服务

服务类型	技术类型	内容及要求
安全运营分析与网络资产梳理服务	服务内容	1.对“三医一张网”现有系统各类安全和重要资产日志信息进行统一收集，并分析研判对发现的威胁进行定位，采取处置措施。对所有跨网访问行为、流量转发状态及安全工具操作日志、NAT 日志进行全量记录，覆盖网络层、业务层、应用层的所有交互行为。日志留存时间需满足行业监管要求，最低留存期限为 180 天。采用旁路部署模式，通过交换机镜像口获取所有跨网流量日志。同时采集防火墙、IPS/IDS 等安全工具的运行日志，具备单独的日志存储资源。 2.提供对卫生专网网络内相关资产进行全方位信息收集整理，梳理卫生专网网络安全工具、网络通信工具、服务器系统、接入终端（含县区单位）、应用系统情况，对各个系统、工具的系统域名、IP 地址、管理员登陆方式等内容做详细登记记录，建立资产安全基线。

工具要求	服务工具	1.采用旁路模式部署，通过接入区镜像口获取所有流量访问日志信息。 2.采集所有安全设备的运行日志、配置日志、流量转发日志、攻击防护日志、NAT 日志，以及所有业务系统的访问日志、操作日志。 3.实时告警规则，对审计发现的恶意访问、非法流量、异常行为开展实时告警，通知运维人员及时处置。 4.溯源分析与场景分析能力，通过收集全网安全设备日志、业务访问日志、流量分析日志，进行统一分析与归类，在发现威胁以及告警后，根据业务访问进行场景分析，快速溯源定位，进行流量取证与应急处置。 5.可根据告警规则，形成自动防御策略，并能够下发给防火墙、IPS 等设备，形成自动联动处置能力。 6.满足公安及网信 180 天日志留存要求，存储资源具备可扩展性，可根据日志量的增长及时完成扩容 7.对全网资产信息进行盘点，形成资产画像。 8.基于全网资产、漏洞信息以及资产风险进行融合分析，直观展示资产的综合安全健康状态，提供合理的优化建议和处置意见。 9.能够全面防护主机系统以及各类终端系统。
服务频率	每月一次	
服务交付物	《安全运营分析与网络资产梳理服务报告》	

11、网络节点变更支持

服务类型	技术类型	内容及要求
网络节点变更支持	服务内容	服务“三医一张网”平台系统。服务期内对网络节点（59 网段、10 网段、172 网段）地址变更及分配约束、网络规划与调优、路由策略、路由协议部署与维护、流量转发规划、高可用性等进行维护服务
服务频率	及时响应	
服务交付物	《网络节点变更支持报告》	

12、应急演练

服务类型	技术类型	内容及要求
应急演练	服务内容	帮助“三医一张网”相关系统制定网络安全应急预案体系。模拟设备故障、链路故障等场景开展高可用性验证，确保路由切换、流量迁移过程不影响业务正常运行。还包含制定相应应急响应组织、预防、预警机制、事件定义分类、应急响应程序、事件上报处理机制、后期处理机制等内容，覆盖演练准备工作、演练环境搭建、演练剧本编写、演练彩排工作、正式演练大会、应急演练总结等各个阶段，帮助实现全面有效的应急演练。
服务频率	每年一次	
服务交付物	《应急演练报告》	

附件 2：网络与信息安全承诺书

网络与信息安全承诺书

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安全和信息安全的行为：

（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）危害电信网络安全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于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。

乙方作为服务提供方，应根据《中华人民共和国网络安全法》第二十二条、第三十六条之规定，履行网络安全保护义务，对其提供的产品和服务的安全负责。因乙方产品设计缺陷、运维不当或安全措施不到位导致网络安全事件的，乙方应承担相应责任。

甲方盖章：

年 月 日