乙方项目编号：

首都医科大学附属北京友谊医院

信息系统运维合同

项目名称：北京友谊医院网络安全运维服务项目

甲方：首都医科大学附属北京友谊医院

乙方：北京同迈科技有限公司

2025 年 9 月 22 日

甲方：首都医科大学附属北京友谊医院

地址：北京市西城区永安路 95 号

联系人：赵现

联系电话：010-63138585

乙方：北京同迈科技有限公司

地址：北京市海淀区北四环西路 66 号 11 层 1210

联系人：郝佳萍

联系电话：13910888244

为维护甲乙双方的合法权益，明确双方的权利和义务，根据《中华人民共和国民法典》及相关法律法规，甲乙双方经友好协商，就乙方向甲方提供系统专业维护服务之相关事宜，签订本合同。

甲方就北京友谊医院网络安全运维服务项目（项目名称）中所需（信息系统名称）专业维护服务，经中技国际招标有限公司（招标代理机构）以 0701-254106140562 号招标文件在国内北京市招标。经评标委员会评定乙方为中标人。甲乙双方同意按照下面的条款和条件，签署本合同。

第一条 维护服务信息

1、乙方向甲方提供信息系统维护服务的名称为：网络安全运维服务项目（以下简称“本项目”）。

2、维护服务期限为：自合同签订之日起 1 年。

3、维护服务费用为：人民币 1,288,039.84 元/年（大写：人民币壹佰贰拾捌万捌仟零叁拾玖元捌角肆分）。合同价款为本合同项下甲方需向乙方支付的全部费用，除此之外，甲方无需因本合同向乙方支付任何费用。

4、本项目的服务清单详见附件一《系统维护服务清单》。《系统维护服务清单》为本合同之附件，为本合同不可分割的一部分，与本合同具有同等法律效力。

第二条 乙方主体资格

1、乙方应向甲方提供签订本合同所需的全部资质文件的复印件，在复印件上注明与原件一致并加盖公章。

2、本合同项下，乙方应向甲方提供的乙方的资质文件为：

☐营业执照；

☐软件产品登记表；

☐软件著作权登记证书；

☐专利证书；

☐系统集成企业资质登记证明；

☐营销人员授权书；

☑售后服务承诺书；

☐产品代理授权书；

☐其他：无。

第三条 付款方式

1、甲方按年支付合同价款，每年分 2 次支付合同价款，具体如下：

☑本合同生效后，甲方向乙方支付合同首付款，人民币 223,124 元（大写：人民币 贰拾贰万叁仟壹佰贰拾肆元 ）；

☑每年的维护期限届满后，乙方没有发生违约行为和质量问题，甲方对乙方的服务满意的，甲方在维护期限届满后，向乙方支付合同尾款，人民币 1,064,915.84 元（大写：人民币 壹佰零陆万肆仟玖佰壹拾伍元捌角肆分 ）；

2、甲方每次付款前，乙方应向甲方提供符合甲方要求的发票，甲方确认发票内容及金额无误后，向乙方支付款项。乙方未提供发票，或者提供发票的内容或金额有误的，甲方有权拒绝支付相应款项且无需承担任何违约责任。

3、乙方账户信息如下：

账户名称：北京同迈科技有限公司

开户行：北京农村商业银行股份有限公司海淀支行海淀镇分理处

银行账号：0413090103000053378

4、甲方开票信息如下：

账户名称：首都医科大学附属北京友谊医院

开户行名称：工商银行珠市口支行营业室

开户行账号：0200003109089210458

纳税人识别号：121100004006886096

第四条 甲乙双方的权利及义务

1、甲方的权利及义务如下：

（1）甲方指定专人负责在本合同执行过程中的组织和协调工作。

（2）乙方的维护服务需要在甲方现场工作的，甲方应免费提供工作场所、必要的软件、硬件、网络、基础数据等条件。

（3）乙方提供的维护服务（☐需要/☑不需要）与甲方院内其他系统进行接口。如须要与甲方院内其他系统进行接口的，甲方应负责参与协调接口协议和参与拟定数据标准。

（4）甲方按照本合同规定的付款方式及时付款。

（5）在任何时候，甲方对乙方负责甲方维护服务的专业人员的主要工作表现不满意，可立即书面告知乙方，并可要求乙方更换人员。乙方应采取合理措施，在收到甲方的书面告知后10个工作日内予以解决。

（6）其他：无

2、乙方的权利及义务如下：

（1）乙方指定郝佳萍为乙方的联系人，协调履行本合同的权利和履行义务。乙方联系人的联系电话为：139 1088 8244 。

（2）乙方应严格遵守本合同及本合同附件一的具体约定向甲方提供专业服务。

（3）乙方应向甲方提供甲方要求的、不涉及乙方保密信息的所有文档及技术资料。

（4）如因乙方原因无法为甲方提供持续的售后服务和产品升级，乙方（☐需要/☑不需要）无偿向甲方提供以下资料，以保证甲方系统的正常稳定运行：

☐源代码；

☐运维手册；

☐数据结构；

☐其他：

（5）乙方应根据本合同的要求安排相应的能胜任的专业人员。在提供服务过程中，乙方保证其参加本项目的人员的相对稳定。

（6）乙方交付的技术服务工作成果应满足网络安全等级保护3级基本要求，并服务过程中或在维保期内需无偿向甲方提供对安全漏洞的修复服务。

（7）乙方（☑需要/☐不需要）向甲方提供年度维护记录。乙方须要提供的，应在每年的维护期限届满后 30 个工作日内，向甲方提供该维护期限的维护记录。维护记录的内容应符合甲方的要求。

（8）其他：无

第五条 售后服务条款及质保服务

1、乙方提供（☐7*24小时/☐5*8小时/☑其他：7×24应急响应，5×8驻场服务）技术支持，并不限支持次数。乙方应根据以下的故障等级提供相应的处理：

故障等级	故障等级定义	处理时间及方式
一级故障	系统瘫痪、严重影响系统使用、严重影响其他关键业务正常使用，如：系统无法访问、数据库无法连接等	立即响应，（☑1小时内/☐__小时内）电话/网络远程支持，并通过最快交通方式到达故障现场，到达现场后4小时内解决故障（因特殊原因无法在4小时内解决故障的，经甲方同意后可适当延长）。
二级故障	影响系统使用、影响其他关键业务正常使用，如：系统能正常访问，但部分功能模块无法使用。	立即响应，（☑2小时内/☐__小时内）电话/网络远程支持，12小时内到达故障现场。到达现场后4小时内解决故障（因特殊原因无法在4小时内解决故障的，经甲方同意后可适当延长）。
三级故障	轻微影响使用，远程支持后可解决；不影响其他关键业务使用，如：系统	（☑30分钟/☐__小时内）响应，（☑2小时内/☐__小时内）电话/网络远程支持并解决故障（因特殊原因无法在2小时内解决故障的，

	自身的BUG，甲方对系统使用的疑问，对系统新功能的咨询等	经甲方同意后可适当延长）。

2、乙方（☑需要/☐不需要）免费为甲方技术人员进行系统管理、操作培训，培训次数不得少于 2 次，具体次数由甲方指定。

3、乙方提供专门技术服务人员，提供每年不少于 30 次的（☑现场/☐非现场）服务，及时检查并处理问题。

4、乙方（☑需要/☐不需要）提供常驻技术支持服务。如乙方须要提供常驻技术支持服务的，乙方应指派 1 名技术工程师常驻甲方。派遣的工程师均应具备相关技术资格认证的工程师，保证提供专业的、正确的和高效的技术服务和技术培训。

5、乙方（☐需要/☑不需要）向甲方提供本合同中所有系统模块的维护、功能和代码的优化。

第六条 知识产权

1、乙方保证甲方及其用户在使用本合同项下产品、服务及其任何部分时，不会受到任何第三方关于侵犯专利权、商标权、工业设计权或知识产权的指控。任何第三方如果提出侵权指控，乙方须与第三方交涉并承担可能发生的一切法律责任和费用。

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。

3、在本合同有效期内，乙方利用甲方提供的知识类资料所完成的知识类成果，归甲方所有。

4、由各方各自独立开发的专利以及其他知识产权归属各自所有。

第七条 保密

保密信息是指甲乙双方各自专有的、或提供给对方的并明确标有“保密”字样的信息，包括但不限于本合同及其签订、许可软件、数据等。甲乙双方承认保

密信息构成有价值的商业秘密。甲乙双方同意严格按照本合同的规定使用对方的保密信息，未经对方的事先书面许可，不得向第三方，或允许向第三方直接或间接地透露保密信息。本合同的保密义务为永久。无论本合同变更、解除或终止，本条款保持有效。

第八条 违约责任

1、乙方应按本合同约定提供信息系统维护服务工作，乙方未能在本合同规定时间内到达现场或解决故障的，每延迟 4 小时，需支付合同总价款 1%的违约金。但因特殊情况，甲方同意适当延长故障解决时间的除外。

2、乙方在接到甲方的维修要求后 24 小时内未能解决故障的，甲方有权指定第三方提供服务，由此造成的额外费用及给甲方造成的损失均由乙方承担。

3、乙方出现违约 3 次以上（含 3 次）的，或者延迟时间累积 24 小时（含 24 小时）时，甲方有权单方解除本合同，并要求乙方支付相当于本合同总价款 20%的违约金。

4、因乙方未按甲方的网络安全要求执行或实施服务，而造成甲方不良网络安全事件、经济损失、恶劣社会影响，每发生一次，乙方应向甲方支付与损失等价的赔偿金，赔偿金额按每起事故不低于合同总款的 5%计算。

5、乙方应确保所提供技术服务的稳健性，因乙方在提供技术服务过程中的过失、疏忽或技术服务工作成果的缺陷，引发的信息系统故障或业务数据损失，而造成甲方经济损失、不良社会影响的，每发生一次，乙方应向甲方支付与损失等价的赔偿金，赔偿金额按每起事故不低于合同总款的 5%计算，同时乙方须按甲方要求积极负责排查故障原因，彻底解决问题。

6、乙方违反保密义务，造成甲方损失的，应支付甲方与泄密内容和不良影响等价的赔偿金，赔偿金额按每起事故不低于合同总款的 60%计算。

7、违约金不足以弥补甲方因此遭受的损失的，乙方还需就不足部分承担赔偿责任。

8、甲方有权从剩余应向乙方支付的款项中优先扣减乙方应向甲方支付的款项（包括但不限于违约金、赔偿金等）。

9、乙方发生违约的，甲方有权要求乙方延长维护期限。延长的维护期限由甲方决定，乙方对甲方提出的延长维护期限有异议的，应提出书面异议并说明理

由。乙方提出书面异议的，甲乙双方通过协商决定延长的维护期限，但延长的维护期限不得低于乙方发生违约行为的合计时长。

第九条 不可抗力

因自然灾害、战争、政府指令、政府主权行为、法律变化等不可预见、不可避免、不可克服的不可抗力事件导致本合同一方当事人无法履行本合同的，受不可抗力事件影响的一方不承担违约责任，但遭受不可抗力一方因延迟履行本合同义务后遭遇的不可抗力事件除外。受到不可抗力事件影响的一方应采取措施将不可抗力事件的负面影响降到最低，否则应对对方当事人的损失扩大部分承担赔偿责任。受到不可抗力事件影响的一方应在不可抗力发生后2日内书面通知对方当事人，并在不可抗力发生后5个工作日内向对方当事人出示不可抗力发生地有权部门出具的不可抗力事件的证明。没有在约定时间内通知对方当事人，给对方当事人造成损失的，负有通知义务的一方应承担相应的赔偿责任。

第十条：信息集成

乙方应确保所提供成果和技术服务满足甲方的信息集成要求：

1、业务字典需通过甲方信息集成平台与主数据系统对接；

2、业务数据要求需按照甲方标准接口定义通过信息集成平台进行对接；

3、信息系统中业务数据需根据甲方需求，支持但不限于数据库同步、视图、接口等集成方式开放；

4、支持HL7 V3、HL7 FHIR等国家或行业标准，以及甲方自定义标准接口对接；

5、支持各类传输访问协议，包括但不限于HTTP/HTTPS、TCP/IP、SFTP、SOAP/HTTP；

6、支持满足安全要求的数据存储及传输的加密/解密；

7、支持根据甲方需要的数据或业务功能提供符合需求的API服务；

8、需按照甲方需求与其它信息系统进行表示、数据、控制、业务流程等方式的集成。

第十一条 国产化适配要求

乙方应按甲方要求无偿进行国产化适配和替代，以确保所提供的信息系统能够在国产操作系统、国产数据库、国产中间件等国产基础软件环境中运行和使用，所有功能保持一致，性能确保稳定，包括服务端和客户端。

第十二条 权利义务的转让

未经甲方事前书面同意，乙方不得将其基于本合同的权利义务的全部或者部分向第三人转让，也不得用以提供担保。

第十三条 合同变更及终止

1、乙方发生以下各项的任何一种情形的，甲方无需催告等其他手续，可直接解除全部或者部分本合同。

（1） 开具的票据或者支票不能承兑，或者陷于停止支付、不能支付的；

（2） 受到监督机构停止营业或者吊销营业执照等处分的；

（3） 申请或者被申请破产、清算、拍卖等任何一种手续及与其类似的其他手续；

（4） 被第三人申请财产保全、强制执行、申请拍卖或者受到其他公权力处分；

（5） 作出解散决议的；

（6） 由于灾害、劳动争议或者其他原因，导致本合同及订单履行困难；

（7） 发生类似前述各项导致经营困难的事由的。

2、甲乙双方可以在取得对方书面同意的情况下，解除本合同或变更本合同。

第十四条 争议解决

因本合同产生的所有争议，甲乙双方应本着诚意友好协商解决。协商无法解决时，任何一方有权向甲方所在地有管辖权的人民法院起诉。

第十五条 其他

1、本合同经甲乙双方的法定代表或授权代表签字并加盖公章后生效。

2、本合同未尽事宜，甲乙双方协商一致后签订书面补充协议。补充协议作为本合同的一部分，与本合同具有同等法律效力。

3、本合同一式 陆 份，甲方执 叁 份，乙方执 叁 份，各份具有同等法律效力。

（本页为签字页，无正文）

甲方：首都医科大学附属北京友谊医院

（盖章）

法定代表人或授权代表

（签字）：

日期：2025 年 9 月 22 日

乙方：北京同迈科技有限公司

（盖章）

法定代表人或授权代表

（签字）：

日期：2025 年 9 月 22 日

附件一：《系统维护服务清单》

序号	名称	服务项	期限
1	网络安全风险评估	风险评估	1 年
2		渗透测试	1 年
3	安全运营服务	威胁情报服务	1 年
4		安全驻场服务	1 年
5		安全培训服务	1 年
6		网络安全检查	1 年
7		网络安全审计	1 年
8		网络安全应急响应	1 年
9		网络安全演练	1 年
10	续订安全产品特征库升级使用授权	防病毒软件使用授权	1 年
11		HTTPS 域名证书使用授权	1 年

附件二：《售后服务方案》

1. 售后服务承诺

售后服务承诺

我司为确保首都医科大学附属北京友谊院信息系统的安全稳定运行，保障医疗业务连续性及数据安全，我司针对本项目作出如下郑重承诺，具体内容如下：

一、服务内容承诺

服务范围：

网络安全风险评估、渗透测试、威胁情报服务、安全驻场服务、安全培训、网络安全检查、网络安全审计、网络安全应急响应、网络安全演练。

续订安全产品特征库升级使用授权（防病毒软件、HTTPS 域名证书）。

服务期限：自合同签订之日起 1 年内，所有服务项同步开展，确保服务无缝衔接。

二、服务响应时效承诺

安全事件响应时效：

工作时间驻场人员实时响应。

非工作时间响应时效如下：

- 紧急事件（如系统瘫痪、数据泄露）：15 分钟内远程响应，2 小时内抵达现场处理。
- 严重事件（如关键系统异常、高危漏洞）：30 分钟内远程响应，4 小时内抵达现场处理。
- 一般事件（如常规告警、配置问题）：1 小时内远程响应，8 小时内完成处理。
- 非事件服务响应：
- 日常巡检、培训、咨询等服务需求：2 小时内响应，24 小时内完成服务交付或安排。
- 服务请求响应：7×24 小时服务热线支持，专人实时接听并记录需求，确

保无遗漏。

三、人员组织及资质承诺

项目团队配置：

项目经理（1 名）：具有 ITSS 服务项目经理、CISAW 风险管理专业级、CISAW 应急服务专业级、高级网络信息安全工程师证书、CISAW 安全集成专业级专业级资质，负责统筹协调、资源调配及进度把控。

服务工程师（2 名）：1 人具备信息系统项目管理师（高级）、CISAW 安全集成（专业级）认证资质、CISAW 安全运维（专业级）认证资质，1 人具备 CISP-CISE（注册信息安全工程师）证书、CISAW 风险评估专业级证书、ITSS-IT 服务工程师资质，提供日常监控、巡检、响应及优化服务。

二线专家团队（≥5 人）：包含攻防专家、合规顾问、应急响应专家，提供技术攻坚、风险评估及重保支持。

保密义务：所有服务人员签订保密协议，未经贵院许可，严禁泄露任何敏感信息。

四、服务质量保障承诺

服务交付标准：

每月总结服务工作，包含风险处置、事件统计、优化建议等。

每季度进行服务质量评估，根据贵院反馈优化服务方案。

技术工具保障：采用行业主流安全设备及自动化工具，确保技术先进性。

合规性承诺：所有服务操作符合《网络安全法》《数据安全法》及等保三级要求，满足合规检查要求。

五、应急处理承诺

制定分级应急预案，覆盖勒索软件、数据泄露、系统宕机等场景，开展实战演练。重大事件期间（如公共卫生事件、监管检查），增派专家团队提供 7×24 小时保障。

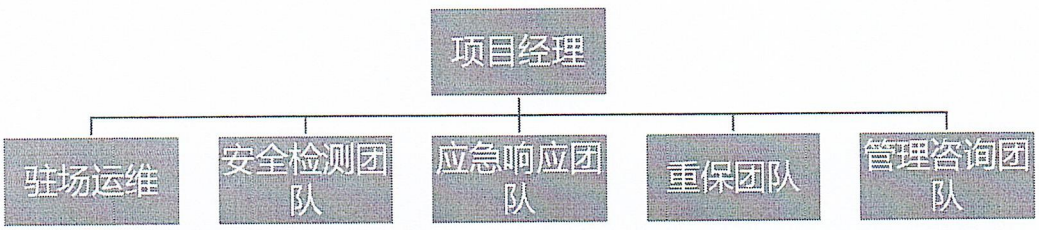
六、沟通与协作机制

设立专属服务对接人，定期召开服务例会，同步工作进展及问题。

建立数字化服务台账，记录所有服务活动及结果，支持随时查阅审计。

企业名称（盖章）：北京同迈科技有限公司
日 期：2025 年　　月　　日

2. 项目组织架构



（一）项目经理主要职责

负责组织项目组成员，制定项目实施目标、计划、方案；

负责项目实施中的的项目组成员具体安排，督促、协调工作；

负责项目阶段成果确认和整个项目的验收工作，提供项目实施总结及验收报告；

根据项目目标与范围，控制项目风险，保证项目质量和进度。

（二）驻场运维人员

（三）安全检测团队

负责本项目中涉及的各项安全检测工作，确保系统在上线前后具备良好的安全防护能力，如：渗透测试、风险评估、互联网暴露面梳理及根据检测过程与结果；

负责编写符合标准规范的检测报告；

对检测过程中发现的问题，提供技术支持与咨询，提供整改建议，并在整改完成后开展复测工作，确保问题闭环处理；

（四）应急响应团队

针对突发的安全事件（如 DDoS 攻击、勒索软件感染、数据泄露、系统入侵等），立即启动响应程序，定位原因、遏制影响、控制事态发展；

对安全事件进行取证与溯源分析，识别攻击来源、攻击手段与入侵路径；

撰写完整的事件调查报告，包括事件经过、影响范围、根因分析、处置过程和改进建议；

（五）重保团队

重要时期保障团队主要在重大活动保障期、系统上线期、节假日、重要会议或国家级活动期间，承担全方位的网络与信息安全保障工作，确保系统安全稳定运行。

（六）管理咨询团队

负责制定并完善项目的网络与信息安全应急响应预案，明确各类安全事件的分级标准、处置流程、责任分工及信息通报机制，确保一旦发生安全事件能迅速响应、有效处置；

依据网络安全法、数据安全法、等级保护等标准，制定符合法规的合规框架。安全策略与体系规划：设计涵盖组织架构、技术防护、应急预案的完整管理体系，包括安全基线配置、访问控制策略等。

3. 项目实施进度计划

序号	任务	工作内容	关键成果	实施时间
1	项目启动	项目启动	项目计划、启动会 ppt	签订合同之日起，具体时间与甲方协商确定
2	项目实施	风险评估服务	《信息资产清单》、《威胁与脆弱性分析报告》、《安全控制措施评估报告》、《信息安全风险评估报告》、《安全整改建议报告》、《符合等级保护要求的安全加固方案》	项目启动会完成后，立即开展该项服务
3		互联网暴露面梳理	《互联网攻击面检测报告》	根据客户需求开展建议：一般在重要保

				障时期之前一个月内开展
4		渗透测试	《渗透测试方案》、《XX 系统渗透测试报告》、《渗透测试跟踪表》、《XX 系统渗透测试复测报告》	根据客户需求开展
5		威胁情报服务 网络安全态势推送	《威胁动态报告》、《安全漏洞情报》、《安全通告月报》、《安全态势年报》	根据客户需求开展
6		网络安全驻场服务	《驻场安全工作周报》	根据客户需求开展
7		防病毒系统巡检和问题排除服务	《防病毒系统巡检报告》、《问题处理跟进报告》	根据客户需求开展
8		可疑样本分析服务	《可疑样本分析报告》	根据客户需求开展
9		安全加固服务	《安全加固报告》	根据客户需求开展
10		安全意识培训	《安全意识培训计划》（明确培训内容、形式、实施安排）、《安全意识培训 PPT 及教材》（提供完整培训课件）、《安全意识测试与考核报告》（评估员工安全意识提升情况）、《培训总结与改进建议》（总结培训效果，并提出后续优化建议）。	根据客户需求开展 建议：一般在重要保障时期之前一个月内开展
11		安全技能培训	《安全培训方案》、《培训课件》、《培训实施记录》	根据客户需求开展 建议：一般在重要保障时期之前一个月内开展
12		网络安全检查	《自查和整改报告》	根据客户需求开展
13		漏洞扫描服务	《漏洞扫描报告》、《漏洞扫描复测报告》	根据客户需求开展
14		网络安全审计	《安全运维审计报告》、《信息安全建设规划方案》及分阶段实施路线图、《安全管理制度汇编》（含应急预案、运维规范等）	项目启动会完成后，立即开展该项服务
15		应急响应	《应急响应与处置报告》、《应急响应预案》	根据客户需求开展
16		重要时期监测	《重保保障方案》、《安全监测日报》、《监测总结报告》	根据客户需求开展
17		网络安全演练	《网络安全演练实施方案》、《网络安全演练总结报告》、《网络安全演练汇报 ppt》	根据客户需求开展 建议在国家、行业的实战攻防演习前开展。

18		防病毒软件使用授权	授权文件	根据客户需求进行授权更新
19		HTTPS 域名证书使用授权	授权文件	根据客户需求进行授权更新
20	项目汇报与总结	项目总结	年度总结报告，报告内容应体现对应急处置工作的科学分析和改进建议。	项目结束实施结束后进行年度总结并进行汇报。

4. 项目管理方案

我司具备专业的项目经理和项目团队，本项目中整体的项目管理工作，我司主要通过：项目进度控制、项目质量保证、项目文档管理、项目风险控制、项目变更管理等内容，根据项目管理的合理性、全面性、可操作性严格执行。

（一）项目进度控制

- 人员保证
- 队伍保证
- 人员考核
- 进度保证
- 进度管理
  - ✓ 工作日报
  - ✓ 工作周报
  - ✓ 建立例会制度
  - ✓ 工作跟踪

（二）项目质量保证

在组织结构上，将设置质量保证小组，专门负责项目过程中“文档质量”和“过程质量”的控制。

质量控制小组由专门的质量保证人员组成。

质量保证小组必须参加项目组的例会，各阶段或里程碑处的评审会议，按计划定期或不定期地对项目的进展情况进行检查，客观地评价项目的实施情况，定期向项目经理和项目领导组汇报检查的内容和情况。

质量管理部也作为项目开发部门和项目领导组之间信息传递的桥梁。

- 项目安全的质量管理
  - ✓ 调研应用安全需求对运行系统可能会造成影响
  - ✓ 工具的使用有可能对运行系统可能会造成影响
  - ✓ 敏感信息泄漏
  - ✓ 对调研结果的争议
- 签署委托评估协议
- 签署保密协议
- 现场评估工作风险的规避
- 安全保密控制
  - ✓ 最小接触
  - ✓ 职业道德
  - ✓ 设备保密
  - ✓ 文档保密
  - ✓ 规范化的实施过程
- 项目质量保证方案

安全服务提供商应对项目实施的各阶段文档进行严格的质量控制和管理，对文档内容的完整性、文字的正确性和语句的通顺进行质量管控。

- 项目质量保证方法
  - ✓ 质量标准的量化
  - ✓ 规范的文档模板
  - ✓ 高效的沟通方式

- ✓ 完整的配置管理

- 项目质量实施控制
  - ✓ 设计评审制度
  - ✓ 质量问题的跟踪
  - ✓ 项目质量管理要求
- 文件记录控制要求
  - ✓ 文件的分类和保管
  - ✓ 文件的编写、审核、批准和发放
  - ✓ 文件的受控
  - ✓ 文件的修改
  - ✓ 文件的领用
  - ✓ 文件的保存、作废与销毁
  - ✓ 文件的保存
  - ✓ 文件的作废和销毁

（三）项目文档管理

- 文档管理要求
- 文件记录控制要求
  - ✓ 文件的分类和保管
  - ✓ 文件的编写、审核、批准和发放
  - ✓ 文件的受控
  - ✓ 文件的修改
  - ✓ 文件的领用
  - ✓ 6. 文件的保存、作废与销毁

（四）项目风险控制

服务项目的主要任务是由驻场服务人员来完成，根据项目特点，项目风险主

要来源于驻场服务人员。通过风险控制措施、服务风险规避措施可有效降低项目实施过程中产生的风险问题，降低风险发生的机率。

在项目过程中可以通过采取以下措施规避风险：

- 签署授权协议
- 签署保密协议
- 现场渗透工作风险的规避
- 规范化的实施过程
- 沟通与交流

（五）项目变更管理

项目变更管理的目的是以一种对于项目影响最小的方式改变现状，项目变更管理内容包括：

- 变更分析
- 变更请求
- 变更控制

（六）项目组沟通机制

- 项目沟通目标
- 项目沟通管理体系
- 项目服务沟通流程
- 项目沟通机制

（七）项目整体管理

项目整体管理包括五个过程：制定项目章程（启动）；制定项目管理计划（计划）；指导和管理项目执行（执行）；监控项目工作和整体变更控制（监控）；结束项目（收尾）

（八）项目人力资源管理

在项目中只有进度、成本和质量三条标准是不够的。另外一条很重要的标准被忽略了，那就是人力因素。许多项目正是忽略了这样一个问题：他们如何组织人力资源会直接影响项目的最终成果。事实上，他们对人力因素的忽略或错误管理会直接影响项目的进度、成本和质量。因此，人力资源在项目管理中与进度、成本预算和质量管理一样重要。事实上，人力因素可以在项目管理中的其他三条标准之间架起协同一致的桥梁。人力因素在保证低成本、快速度和高质量地完成项目的过程中发挥着重要的整合作用。项目管理中的人力资源管理把人力当作完成项目的一个核心因素，同时管理人力因素不能采用机械的、程式化的方式。人力因素并不比项目管理中的硬件更重要。项目经理必须认识到二者的同等重要性。这就要求在项目管理传统的成本、进度和质量三条标准之中增加一条：人力。

（九）项目组织规划

组织规划就是确定项目管理需要的角色，各角色应负的责任以及诸角色之间的从属关系，组织规划的依据。制定项目管理团队的组织规划要从项目的具体情况出发，综合考虑以下一些因素：

- 项目同其他组织的联系。
- 项目管理人员的要求。

（十）项目闭环管理

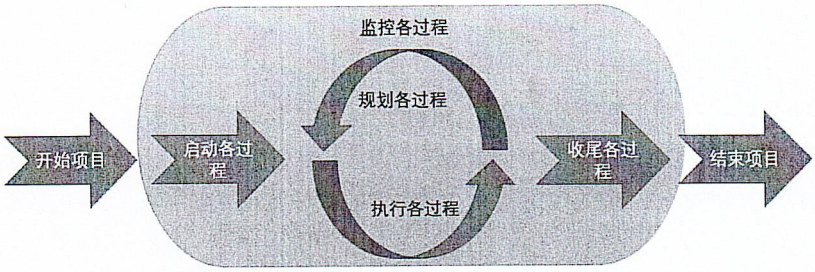
我司在多年项目管理中得出经验，我司融入科学的闭环流程模型，将工作开展过程中发现问题到处置问题形成闭环机制，使友谊医院可以得到有效反馈，高效的完成服务项目有效规避中安全风险。

项目管理人员在项目运行过程中对项目进行监控和管理，通过对相关项的偏差分析，发现、预测、分析项目过程中可能存在的风险或瓶颈，然后提前规避，或者提前想好应对策略，让项目始终处于可控状态。

（十一）项目管理闭环模型

针对网络安全工作开展过程中发现的安全风险进行实时跟踪、定期验证，从

整体的信息安全运行角度出发对安全检查过程中发现的网络安全风险开展闭环检测，形成相应的问题记录单、整改情况记录单、问题反馈记录单，并以月报的形式向用户开展工作汇报，以期将安全检查过程中发现的网络安全风险在事件发生前完成漏洞的整改建议工作。项目的全生命周期一般按照项目的启动、计划、执行、监控和收尾五大过程组运行，这一过程的监控环节其实就是一个闭环——项目在计划和执行的环节中，通过监控来发现计划和实际的偏差，并根据反馈的结果修正，直到收尾后退出该循环，如下图：



图：项目管理闭环模型

不断地对项目个环节进行偏差修正，可以减少变更带来的负面影响，保质保量地完成项目。

（十二）项目成本管理

成本控制，是根据项目一定时期预先建立的成本管理目标，由成本控制在由成本控制主体在其职权范围内，在生产耗费发生以前和成本控制过程中，对各种影响成本的因素和条件采取的一系列预防和调节措施，以保证成本管理目标实现的管理行为。实施阶段的成本管理与控制是建设项目成本发生的主要阶段，通过确定成本目标并按计划进行实施、资源配置，如何对项目发生的各种成本费用进行有效控制。

- 人员成本控制
- 全过程控制
- 目标管理控制
- 成本管理控制

（十三）项目保密管理

- 安全保密措施
- 保密知识培训
- 安全制度培训

附件三：《运维服务方案》

1. 安全运营服务方案

1) 威胁情报服务

微步在线威胁防御系统(Security Intelligence Gateway，以下简称 OneSIG)是一款帮助企业自动化抵御威胁的防御产品。该产品基于专业、成熟的高性能网关技术，通过透明串行部署或旁路部署在网络中，在保证对网络零影响的基础下，实现网络威胁的实时发现和阻断。对外，OneSIG 通过入侵防护引擎检测并阻断包括 0day 攻击、webshell 攻击、反序列化攻击、病毒攻击等多种网络入侵攻击；对内，OneSIG 通过情报防护引擎，结合高精度的威胁情报自动阻断企业内部失陷主机的恶意回连行为，帮助企业有效解决钓鱼、勒索、挖矿、APT 攻击以及常见僵木蠕行为。同时 OneSIG 基于高性能网关技术和开放的联动性，支持数十万条的封禁策略添加，可实现千万级别的 IP 封禁，帮助友谊医院实现网络威胁的全面防护和威胁闭环。

2) 网络安全态势推送

奇安信具有一批专业的安全服务队伍，非常注重对最新安全技术及安全信息的发现和追踪，并通过服务的平台与客户及时交流，帮助客户保持领先的安全理念和技术。我司会为客户提供定期的安全信息通告服务，安全信息中会包括最新的安全公告，病毒信息，漏洞信息等内容。

客户可以根据收到的安全预警通告来防范病毒的攻击和黑客的入侵，可以在第一时间得到漏洞的修补方法，以防止安全事件发生。

安全通告服务以邮件、电话、走访等方式，将安全技术和安全信息及时传递给客户。

方法与流程

- 业界动态
- 国家安全政策及法律法规

- 漏洞信息
- 安全产品评测信息
- 病毒信息
- 工作方式
- 邮件通知
- 在线通告

工作输出

《安全漏洞情报》、《安全通告月报》、《安全态势年报》

3) 安全驻场服务

- 服务目标
  - ✓ 根据服务目标和服务方案，完成安全运维服务
  - ✓ 定期输出各种报告

4) 防病毒系统巡检和问题排除服务

防病毒系统巡检和问题排除服务，由安全服务工程师进行现场提供。主要针对医院现有的防病毒软件和主机安全防护系统进行巡检，分析发现系统的控制台以及各个终端客户端程序的运行状态。同时，针对自定义的扫描策略和定期计划进行核实，确保按期进行任务下发。以及针对防护系统中的日志进行综合分析，发现日常系统的运行缺陷，通过策略调整等方式进行运行优化。同时，结合医院现有的安全防护设备和系统，分析病毒的来源以及传播路径等情况，针对此暴露的安全隐患进行安全加固。通过策略的联动处置，在一定程度上切断病毒的传播路径和封堵进入口，提升医院的防护能力。

5) 可疑样本分析服务

由一线服务人员跟医院技术负责人沟通获取可疑样本，通过初步分析判断后将样本提交到二线安全专家进行分析研判。安全专家针对可疑样本进行综合分析，最终确认是否包含恶意代码。如研判没有恶意代码，那么该样本定性为产品误报。

一线人员通过策略白名单进行处理，并沟通厂商进行特征更新。如研判存在恶意代码，那么该样本定性为恶意。一线人员通过策略黑名单进行处理，并沟通厂商更新特征库。

6） 安全加固服务

根据渗透漏扫测试结果，公司针对所发现的安全问题，提供安全加固支持服务及对应的专家咨询并提出可操作性强、效果佳的系统安全加固建议。。

提供远程服务支持，可按医院要求提供现场支持服务，同时我司可按医院需要，提供现场安全加固服务。

安全加固工作主要以人工的方式实现，具体内容如下：

a） 信息收集

b） 系统备份

c） 系统加固

d） 配置复查

e） 应急恢复

安全加固和优化服务存在以下安全风险：

- 安全加固过程中的误操作；
- 安全加固与业务应用系统冲突，安全加固后造成目标主机、设备和网络的资源消耗，导致业务服务性能下降、服务中断；
- 厂家提供的加固补丁和工具可能存在新的漏洞，带来新的风险。
- 漏洞盒子将采取以下措施，控制和避免上述风险：
- 制定严格的安全加固计划，充分考虑对业务系统的影响，实施过程避开业务高峰时段；
- 严格审核安全加固的流程和规范；
- 严格审核安全加固的各子项内容和加固操作方法、步骤，经医院同意后方可进行；

- 制订意外事件的紧急处理和恢复流程；
- 所有的安全加固程序和安全加固操作经过事先验证。

7） 安全培训服务

国内各部委、政府部门、企事业单位对攻防技术培训服务的需求近年来不断增加。作为网络安全人才培养方式的一个重要组成部分，攻防技术培训需求越来越多的被各个组织单位提出。

为友谊医院培养了解、熟悉安全技术相关理论知识与实际操作的人才。通过培训与考试，为友谊医院选拔优秀安全技术人员。

- 课程内容列表

培训内容如下，具体以与用户方沟通确认后为准：

序号	培训内容	培训材料
1.	常见漏洞及解决方案	《培训 PPT》
2.	相关工具	
3.	事件处置手册等	
4.	重要应用系统安全配置	
5.	主要安全设备的原理及安全设置	
6.	红蓝对抗中主流技术手段	
7.	常用工具	
8.	攻击思路	
9.	检测方式	
10.	紧急事件处理方法以及安全意识	
11.	新技术引入导致的安全问题等	
12.	服务方法	

- 培训交付物

包括但不于培训材料、培训记录。《安全意识培训计划》（明确培训内容、

形式、实施安排）、《安全意识培训 PPT 及教材》（提供完整培训课件）、《安全意识测试与考核报告》（评估员工安全意识提升情况）、《培训总结与改进建议》、《安全培训方案》、《培训课件》、《培训实施记录》。

8） 网络安全检查

- 迎检服务
  - ✓ 交付物：《自查和整改报告》
- 漏洞扫描服务
  - ✓ 资产识别与梳理
  - ✓ 漏洞扫描执行
  - ✓ 漏洞分析与分类
  - ✓ 报告输出与风险建议
  - ✓ 交付物：《漏洞扫描报告》、《漏洞扫描复测报告》

9） 网络安全审计

- ✓ 交付物：《安全运维审计报告》、《信息安全建设规划方案》及分阶段实施路线图、《安全管理制度汇编》（含应急预案、运维规范等）。

10） 网络安全应急响应

我司应急响应服务，以“快速响应、力保恢复”为行动指南，致力于成为网络安全领域的 120 急救中心，通过在遇到突发安全事件后采取专业的安全措施和行动，并对已经发生的安全事件进行监控、分析、协调、处理、保护资产等安全属性的工作，保障企业用户的网络安全，最大程度的减少安全事件所带来的经济损失以及恶劣的社会负面影响。

- 应急响应方式

  应急呼叫方式：我司应急响应服务支持两种接入方式，20 分钟内响应：

  - ✓ 7*24 小时应急热线支持，应急服务热线：95015；

✓ 微信支持：微信支持线上建单。

应急服务方式：我司应急响应服务方式分为现场应急与远程应急服务，应急人员接单后， 2 小时内现场处置。

防止事件继续扩散，限制了潜在的损失和破坏，使目前损失最小化；对其它相关业务的影响是否控制在最小。

✓ 应急响应交付成果

提供各种信息安全的应急预案；双方商定应急预案启动机制；完成应急响应后提供包括但不限于应急响应报告、处理结果、总结建议等。

11）重保保障

在重保各阶段，协助友谊医院完成重保的防护任务，在出现网络安全事件时，能够在第一时间进行处置，将网络安全风险降至最低。

✓ 完成保障前检查、隐患排查、内容检查等准备工作及整改；

✓ 保障期间完成重大安全事件预警与通告、对甲方系统的进行完整性检查、对网站可用性进行监测，发生问题及时进行处置；

✓ 保障结束后对防护期间发现的问题及应对方案。

● 保障方案设计

重保方案设计应根据重大活动或者会议安全关注侧重点，根据以往重保经验、重保能力需求分析、重保工作的队伍组建情况以及调研结果，结合重保期间可能面临的安全风险，采用积极防御体系建设和主动安全运营机制的工作思路，形成的重保服务的网络安全保障设计实施方案。方案中要明确有效的安全产品、安全措施、安全服务、安全管理流程和安全保障机制等，同时根据信息系统开发及实际运行环境部署实施计划，制定合理的网络安全实施方案，明确在不同阶段的主要工作内容、人员投入、实施计划和风险控制措施，将重保工作内容分为备战、临战、实战、决战四个阶段服务。

重保方案设计主要由客户安全专家以及重保支撑团队编制完成重保方案的设计与实施，由客户安全专家与重保重要单位负责人以及重保支撑团队依据现场实际环境对方案进行评审，以评审结果为标准逐步落实重保工作，确保后期重保工作的有效实施。

12) 网络安全演练

实战攻防演习是有目的、有组织的活动，通过组织攻击队、防守单位对实际环境的攻击，以达到检验参演单位的防守能力、分析参演目标系统的安全风险、最终提升安全防御能力的目的而开展的演习。实战攻防演习方案设计是根据实际演习中各参与方所需完成的工作，围绕既定目标，按照共同参与，攻防兼备的原则，对攻防演习工作各环节展开描述。

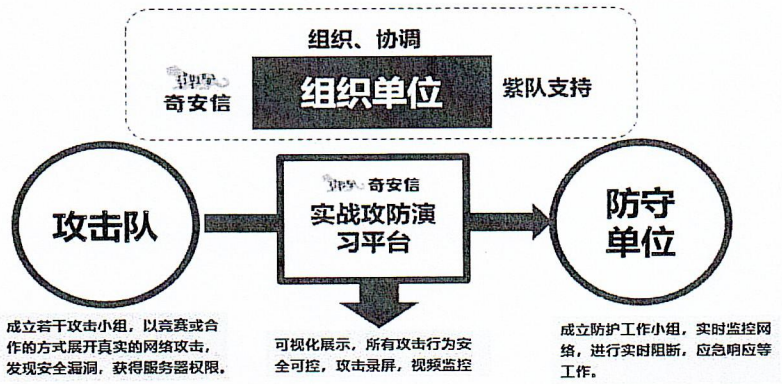


图 攻防演习架构图

整个演习工作由演习主办单位对全局进行把控协调，攻击组和防守组按照演习约定分别对演习目标开展真实的攻击和阻断防护。

13) 续订安全产品特征库升级使用授权

- ✓ 提供防病毒软件使用授权
- ✓ 提供 HTTPS 域名证书使用授权

附件四：《中标通知书》

中技国际招标有限公司

CHINA INTERNATIONAL TENDERING LIMITED COMPANY

编 号 Ref. No.： ITCYW-6

日 期 Date： 2025 年 8 月 20 日

发 件 人 From： 马建

致：北京同迈科技有限公司

北京友谊医院网络安全运维服务项目

（招标编号：0701-254106140562）

中标通知书

关于标题项目，经评标委员会评审，并经采购人审批同意，兹通知贵单位在如下内容的招标采购中中标：

包号	品目号	标的名称	数量	中标金额（人民币元）
1	1-1	网络安全运维服务	1 项	1,288,039.84

请贵单位于本通知书发出后 3 日内与采购人联系，在本通知发出后 30 日内签署采购合同，采购合同签署后将合同扫描件发送至邮箱：majian4@cgci.gt.cn，我司将在收到合同扫描件后 5 个工作日内将投标保证金原路退回。

采购单位：首都医科大学附属北京友谊医院

采购人联系电话：010－63139390

我公司地址：北京市丰台区西营街 1 号院通用时代中心 C 座 9 层

联系人：马建　　联系电话：81168697

谢谢参与！

中技国际招标有限公司

2025 年 8 月 20 日

抄送：首都医科大学附属北京友谊医院