网络安全运维服务项目合同

甲方：北京中医医院顺义医院

乙方：北京金瑞亿科技有限公司

就乙方受甲方委托为甲方提供安全运维服务事宜，双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，共同拟订并签署协议如下，并由双方共同恪守。

第一章　总则

第一条　定义和解释

1. 维保服务：网络安全运维服务

第二条　合同期限

服务期三年，合同一年一签，如不符合医院评核与续签条件，医院将不予续签下一年度合同。本年为服务期第一年，自合同生效之日起计算。合同有效期：本合同由合同双方法定代表人或授权代表签字并加盖公章之日起生效；有效期一年。

第三条　合同前提

乙方确认，双方订立本合同的前提是基于：(1)乙方是依法成立并有效存续、声誉良好的法人实体，并具备履行本合同的相关法律资质；(2) 乙方所提供的相关维保服务是可靠的、完整的、符合国家相关技术标准的，且能够满足本合同及相关文件中的承诺及要求。

第四条　合同解释顺序

本合同正文及附件之间如出现条款解释冲突，应按如下顺序进行解释：

1. 合同附件；

2. 合同正文中划线部分；

3. 合同正文中非划线部分。

第二章　服务内容、方式及期限

第一条　服务范围、内容及方式

1.维保服务范围：网络安全运维服务；

2.维保服务内容及要求：

2.1 维保服务内容

服务名称	服务频率	备注
集成运维巡检	12 次/年	全年 12 次，每月 1 次
威胁情报分析	12 次/年	全年 12 次，每月 1 次
脆弱性检查服务	2 次/年	全年 2 次，每半年 1 次
安全加固服务	2 次/年	全年 2 次，每半年 1 次
差异化分析服务	1 次/年	全年 1 次
网络安全检查	全年	根据甲方要求
风险评估服务	1 次/年	全年 1 次
安全管理体系建设	1 次/年	全年 1 次
渗透测试服务	4 次/年	全年 4 次，每季度 1 次
应急响应	全年（含应急预案完善）	根据实际情况提供应急响应服务（包含应急预案完善）
应急演练	1 次/年	全年 1 次
重保值守服务	全年	重保期间值守服务
安全培训	1 次/年	全年 1 次
驻场运维服务	1 人/年	全年 1 人次，工作日 5*8 小时值守
设备资产管理、配置	全年	根据甲方要求
网络调整优化	全年	根据甲方要求
操作系统调整优化	全年	根据甲方要求
设备维护更换、优化	全年	根据甲方要求

2.2 服务要求

2.2.1 集成运维巡检

针对甲方的安全设备、服务器、网络设备、虚拟化、存储等硬件设备，健康状态提供深入、全方位巡检服务。对相关网络设备、服务器的日志进行分析，进

行定期的安全维护服务，包括：设备 CPU、内存、磁盘容量状态，日志审计分析、连通性测试等，定期修改网络设备、服务器登录用户名及口令等，备份网络设备、服务期配置。做好版本管理，形成工作日志、维护报告。

2.2.2 威胁情报分析

（1）分析目标和范围：确定需要保护的资产、威胁的来源和类型等，以便有针对性地进行情报收集和分析。

（2）数据收集和整合：从网络流量、日志文件、外部情报获得数据支持，对收集来的数据进行整合。

（3）数据预处理和筛选：在收集到大量数据后，进行预处理和筛选工作，去除无关或重复的信息，提取出有价值的威胁情报。

（4）威胁情报分析：分析包括关联分析、趋势分析、漏洞分析等，目的是找出潜在的安全威胁、攻击手段和来源等信息。

（5）威胁预警和响应：基于威胁情报分析的结果，可以发出威胁预警，及时告知相关人员可能的安全风险。同时，制定相应的响应措施，如修复漏洞、升级软件、调整安全策略等，以降低潜在的安全风险。

2.2.3 脆弱性检查服务

通过专业的检测工具和分析手段，从技术层面分析网络安全技术架构、网络、安全设备性能和策略、主机（包括操作系统、数据库和中间件）安全策略方面所存在的安全隐患，为后续信息系统安全加固提供客观数据，减少信息安全隐患，提高网络和系统安全防护能力。

2.2.4 安全加固服务

乙方需根据信息系统进行的漏洞扫描服务结果为依据，结合信息系统的安全特殊需求和业务流程制定安全加固方案，在不影响当前业务开展的前提下，对信息系统内的操作系统、数据库、安全设备以及中间件的安全配置策略进行加固，及时消除因安全漏洞被恶意攻击者利用从而引发的风险、整体上提升业务信息系统抗风险能力。

2.2.5 差异化分析服务

针对甲方的系统从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设

管理、安全运维管理等 10 个方面进行差异化分析。

2.2.6 网络安全检查

根据上级工作要求和甲方自身安全需求，提供必要的人员和技术支持协助甲方完成各项网络安全自查和整改工作。配合甲方完成上级监管部门的信息安全检查，确保甲方信息系统符合国家及行业安全合规要求，并有效降低安全风险。服务提供方需在迎检过程中提供全面的技术支持，包括资料准备、风险评估、检查陪同、问题整改及优化，确保顺利通过检查，并提升甲方整体安全防护能力。

2.2.7 风险评估服务

结合甲方网络安全现状，对甲方进行现场安全风险评估，评估网络安全技术和管理体系的有效性，发现网络安全全局性或者局部性重大风险。包括但不限于网络基础设施规划方案、安全设备和安全产品部署、安全策略、安全运营情况等相关安全措施的合规和有效性,评估结果形成报告。协助对发现的问题进行确认、整改。

2.2.8 安全管理体系建设

乙方针对等级保护三级要求的安全管理制度文件、提供符合三级系统要求的整套制度文件。协助甲方完善并加强日常运维相关信息业务系统的安全规定、制度和流程。协助甲方完成三级等保测评工作，直到甲方顺利完成相关信息系统的等级保护工作。

2.2.9 渗透测试服务

在甲方的授权和监督下，对信息系统进行受控的、非破坏性的远程安全检测，查找存在的安全隐患，并针对安全隐患提出解决办法，切实保证信息系统安全。检测内容包括：跨站脚本漏洞、主机远程安全、残留信息、SQL 注入漏洞、系统信息泄露、弱口令等。

2.2.10 应急响应

乙方针对甲方可能发生的不同类型的安全事件、设备故障等突发事件时，根据故障的类型和严重程度，迅速调配相应的资源和人员。发生突发事件时，乙方能够在第一时间迅速响应，立即启动应急预案，30 分钟速度赶赴现场，对突发事件进行全面评估和诊断，采取有效的处置方法，2 小时恢复系统运行。应急响应结束后，为甲方提供详细的事件报告，深入分析事件发生的原因、处理过程和经

验教训，提出针对性的整改建议。应急服务时间为 7*24 小时。

2.2.11 应急演练

乙方应对甲方网络环境、业务流程、关键数据和潜在的安全风险，协助甲方制定一套专业的网络应急演练。演练结束后，要对演练结果进行全面评估和总结，分析演练过程中存在的问题和不足，提出针对性的改进建议。对应急预案进行修订和完善，确保其更加合理、有效。

2.2.12 重保值守服务

确保甲方在重大活动、重要会议、关键业务运行期间的信息系统安全稳定运行。服务提供方需在重要时期内加强安全监测，覆盖网络、主机、应用、威胁情报、日志分析等多个维度，做到实时预警、快速响应、闭环处置，有效降低安全事件发生的概率，确保业务连续性。

2.2.13 安全培训

通过系统化的信息安全意识培训，提高甲方单位员工的网络安全素养，增强其对常见安全威胁（如钓鱼邮件、社工攻击、恶意软件等）的识别能力，降低因人为因素导致的信息安全事件风险。本服务涵盖基础培训、模拟演练、案例分析及互动教学，结合行业最佳实践，提供定制化培训方案，确保培训效果可量化、可落地。

2.2.14 现场值守人员服务

需派遣至少 1 名安全技术人员进行现场值守服务，针对甲方的信息安全体系中各类安全设备和系统的综合运维服务。现场值守人员需提供日常安全设备运行维护服务以及安全风险监控和处置，包含日常运行问题发现和处置、安全设备和系统的策略优化、日志分析、安全事件处置等工作。及时将重大安全问题反馈至后端团队。

现场值守服务时间：每周不少于五天，每天不少于 8 小时。现场值守人员应具有信息安全 3 年以上工作经验，如现场值守人员离职或请假，由乙方安排一名具备同等能力或更强能力的人选，且中途不能有空档期。

2.2.15 设备资产管理、配置

针对甲方的硬件资产进行精准梳理和详细记录。无论是服务器、网络设备、虚拟化等硬件设施，建立起完善、清晰的设备台账、标识，实现资源的高效利用

和优化配置。明确每一项资产的详细信息，甲方能够清晰掌握自身的资产状况，避免因配置信息混乱导致的系统故障和安全漏洞。

2.2.16 网络调整与优化

通过甲方网络环境、拓扑图和流量的使用情况，找出可能存在的故障、丢包率、传输路径过长等问题，对网络进行合理的配置和调整，优化网络拓扑结构。根据甲方提供的不同应用或用户分配合理的带宽、IP 地址，确保满足甲方需求。要统一管理、分配、记录 IP 地址的使用情况。

2.2.17 操作系统调整优化

由于操作系统的软件冲突、病毒攻击等诸多因素，系统难免会出现各种故障，乙方能够快速准确地诊断和解决系统故障，确保系统的稳定和数据的安全。

精通各类操作系统，包含 Windows、Linus、欧拉、虚拟化等，了解甲方的使用场景、具体需求，调整、配置或安装操作系统。

2.2.18 设备维护更换、优化

对发生故障的硬件设备由甲方提供需要更换或增加的配件，乙方协助甲方完成更换或安装，故障修复完成后，要对设备进行全面的测试，确保设备恢复正常运行。

2.2.19 医院现有虚拟化 4 套（含服务器 115 台），实体服务器 118 台，网络交换机 448 台（其中内网 321 台，外网 127 台），安全设备 45 台。

3.其他要求：

3.1 甲方集成运维涉及繁多的硬件设备、存储、网络、虚拟化等多个领域，需要经验丰富、责任心强、高效执行的专业人员来完成这项工作。从专业匹配和工作专注度的角度出发，集成运维需单独派遣相关专业人员负责。

3.2 甲方在运维期间对部分运维服务内容提出变更，乙方经过分析、评估后，未超出合同规定的范围，乙方应按变更后的服务内容履行。

3.3 现场值守人员需要在工作日对甲方所有机房巡检，巡检内容包含服务器运行状态、磁盘占用情况、CPU、内存使用情况等内容。每月要完成对甲方所有楼层弱电间巡检留存巡检记录。

3.4 提供专人对接医院，提供专线电话以满足 7×24 小时应急保障需求，协调技术资源以满足本项目各项服务需求。

3.5 服务内容中的技术服务、现场值守人员等，乙方均需自行提供，不得进行转包、分包等。如未经甲方同意，进行转包或分包，一经发现，甲方有权无条件解除合同，同时乙方需赔偿甲方相关损失。

3.6 防病毒产品策略优化，针对近期安全风险威胁情报对防病毒软件策略进行优化，对日常运维中出现的疑似误杀样本进行威胁分析，并根据分析结果提供解决方案。

3.7 为保障相同问题快速处理，业务快速恢复，运维周期内乙方需提供运维知识库管理系统给甲方免费使用。如非乙方自有知识产权，乙方需提供运维知识库管理系统著作权厂商针对本项目的原厂售后服务承诺函并加盖原厂公章。

3.8 为提升运维效率，优化资源管理，增强风险预警等方面，运维周期内乙方需提供运维管理软件给甲方免费使用。如非乙方自有知识产权，乙方需提供运维管理软件著作权厂商针对本项目的原厂售后服务承诺函并加盖原厂公章。

3.9 为便于甲方对机房内设备进行统一登记管理，运维周期内乙方需提供数据中心资产管理系统软件给甲方使用。如非乙方自有知识产权，乙方需提供运维管理软件著作权厂商针对本项目的原厂售后服务承诺函并加盖原厂公章。

第三章　费用及付款

第一条　合同价格

1.本次合同为服务期第一年，本合同项下乙方提供的全部服务费用合计人民币【418,000.00】元（大写人民币：【肆拾壹万捌仟元整】），此为含税金额。本合同约定的 服务费用 的增值税税率为【6%】；其中不含税价款（精确到小数点后 2 位）共计（人民币大写）：叁拾玖万肆仟叁佰叁拾玖元陆角贰分；（小写）：¥394,339.62，增值税（精确到小数点后 2 位）共计（人民币大写）：贰万叁仟陆佰陆拾元叁角捌分；（小写）：¥23,660.38。履行本合同涉及的一切税费的税率、费率执行国家税收政策。若国家税收政策发生变化，则本合同涉及的相关税费根据国家政策的调整而调整，但本合同约定的价税合计金额保持不变。

2.上述价格包括但不限于乙方提供的服务及其他服务所需的全部费用。除本合同约定的费用外，甲方不再为乙方履行本合同项下义务向乙方支付任何税、费。

3.甲方只负责支付合同约定的全部服务费，运维期间产生的其他费用全部由

乙方支付。

第二条　付款条件

甲方付款方式采用分期支付形式，甲方合同期内将分 2 次向乙方支付费用，具体支付条件如下：

（1）首付款：合同签订生效后，乙方为甲方提供服务满六个月且服务符合约定标准的，甲方向乙方支付合同总金额的 50%。，即人民币 209,000.00 元（大写人民币：贰拾万玖千元整）。

（2）尾款：合同期满验收合格后甲方向乙方支付合同剩余的 50%，即人民币 209,000.00 元（大写人民币：贰拾万玖千元整）。

本合同下甲方每次付款前，乙方均应至少提前 7 个工作日向甲方提供当次支付金额全额的正式增值税专用发票，需对该发票进行检验盖章后送达甲方，否则甲方有权延迟付款且不视为违约。因乙方未及时送达合格的增值税专用发票或因其他乙方原因导致甲方无法抵扣进项税的，乙方应及时积极协助甲方办理相关补救手续，并赔偿甲方的相应损失。

如因涉及财政资金管理，如预算批复，财政支付系统调整等原因，甲方有权调整支付时间，且无需承担违约责任。

第三条　支付方式及发票约定

1.支付方式采用银行转账付款，乙方确认收款账户信息如下：

户　　名：北京金瑞亿科技有限公司

开 户 行：中国建设银行北京大兴支行

银行账户：11001009000053017588

纳税人识别号：91110115069638774B

发票条款：

（1）甲方确认开票信息如下：

发票抬头：北京中医医院顺义医院

统一社会信用代码：121101104009441667

地址、电话：北京市顺义区健盛街 1 号院

开户行及账号：北京银行顺义支行

（2）乙方向甲方开具的发票不作为甲方已经完成付款的凭证，甲方相应款项到达乙方指定账户视为完成相应的付款义务。

第四章　服务承诺及验收

第一条　运维服务标准

1.乙方应组建项目服务小组，并指定固定联系人，提供本合同约定维保服务期内的立即响应服务，30 分钟内赶赴现场，2 小时内恢复运行：甲方可随时联络乙方的服务团队，以便咨询诊断与本合同相关的事项，保证软件的安全稳定运行。

2.乙方在提供网络安全服务的过程中，要严格遵守合同规定，执行《中华人民共和国保守国家秘密法》、《中华人民共和国个人信息保护法》及有关保密的法律法规，服务过程中凡是涉及的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

3.乙方应保证提供给甲方的服务事项符合《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等相关法律法规及行业惯例规定的安全标准，不存在任何影响网络及信息安全的安全缺陷、漏洞等。

4.乙方在开展的网络安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，应对风险进行说明。

第二条　运维服务责任

1.如乙方经甲方通知后在约定期间内不能按照上述约定及时履行义务的，甲方有权另行委托任何第三方进行运维，由此导致的运维费用由乙方承担，甲方有权直接向乙方追偿并要求乙方承担违约责任。

2.乙方未按照本合同约定提供专业技术人员团队，或擅自更换人员的，经甲方通知后，应及时予以改正，经甲方通知后仍不改正的或上述情况累计发生 3 次以上的，甲方有权解除合同。如因此给甲方造成损失的，由乙方承担全部赔偿责任。

第三条　运维服务验收

双方确定以下列标准和方式对乙方的运维服务工作成果进行验收（详见附件 2:验收考核细则）：

1.乙方服务完成后，确保甲方网络设备的系统、漏洞、病毒库等升级到最新，

硬件设备无报警、损坏等。

2. 乙方在完成全部约定的运维服务后，须将服务过程中形成的各类运维报告（包含但不限于集成运维巡检报告、威胁分析报告、脆弱性检查报告、安全加固报告、差异化分析报告、渗透测试报告、应急预案、应急响应报告、驻场运维报告等）进行系统梳理，并整理汇编为规范的成果文档，提交甲方审核。

3. 运维服务期满后，乙方完成全部需求且系统运行稳定。

4. 现场值守人员应服从甲方统一的工作安排，严格遵守作息时间，工作期间不得从事其它活动；严格遵守甲方的规章制度和保密制度。

5. 配合甲方及测评公司完成三级等保测评工作，直到测评公司出具报告为止。

6. 乙方完成漏洞扫描等检测软件的修复验证工作，且无遗漏。

7. 最终验收：运维服务结束前且无出现重大缺陷，甲方开展竣工验收工作，出具详细的验收报告文件。不符合甲方验收要求，甲方有权中止合同

第四条　甲方权利义务

1. 本合同有效期间，甲方依约配合乙方完成其承担的合同义务。

2. 在乙方履行相应义务后，甲方依约支付合同费用。

第五条　乙方权利义务

1. 乙方有权要求甲方依约支付合同费用。

2. 乙方有权要求甲方为履行合同义务提供必要协助。

3. 乙方为甲方提供项目服务人员，未经甲方同意乙方不得随意变更本合同中所载的项目服务人员，如项目服务人员出现离职、疾病等确实无法继续为甲方提供服务情形的，由乙方安排一名具备同等能力或更强能力的人选，且中途不能有空档期。

4. 乙方已知悉并保证所有服务人员均应遵守甲方相关制度规定，未经甲方允许不得进入与运维服务无关的场所。

5. 乙方工作人员应持续具备相应资质、能力，所提供的服务和使用的零件或材料等应符合国家、行业相关标准及水平。

6. 乙方工作时应确保甲方的物品和设备完好无损。乙方应确保乙方工作人员、甲方人员及其他第三方人员的人身和财产安全，否则由此所造成的一切损失全部由乙方承担。

7. 乙方在工作期间，应采取完备的安全保障措施，应对工作人员进行安全教育，作业期间禁止饮酒、吸烟及大声喧哗等。

8. 乙方在工作期间，应严格遵守甲方的规章制度，并严格按照操作规程工作。

9. 若作业过程中需要相关证件，由乙方人员负责办理，并将证件资料于甲方处备案。

第五章　知识产权及保密

第一条　知识产权及保密

1. 双方应对本合同履行过程中所知悉的知识产权、商业秘密、技术成果、经营计划和战略、客户信息及其它非技术性信息承担保密义务。未经揭露方书面同意，不得向社会公众或其他方通过任何途径出示、泄露，不得对上述信息进行复制、传播和销售。双方同时应约束其员工履行保密义务。

2. 在本协议有效期内以及在有效期后的一年内甲乙双方均不得将合同及项目相关的技术资料、技术秘密等成为公共信息之前披露给任何其他方，依照相关法律法规的规定，或者有权机关、监管机构、一方上市的证券交易所的要求而进行披露的除外。

第六章　违约责任

第一条　违约责任

1. 若因乙方原因在规定期限内不能按时履行义务的，则每延迟一天，乙方需向甲方支付合同总金额 1%的违约金，但此项违约金数额累计不超过合同总金额的 30%。延迟达到 15 日，甲方有权解除合同，乙方还应赔偿由此对甲方造成的损失。

2. 在乙方履行相应义务的前提下，因甲方过错在规定期限内不能按时付款，则每延迟一天，甲方需向乙方按照未付款部分日万分之五的违约金，但此项违约金数额累计不超过合同总金额的 30%。

3. 乙方应独立完成本合同约定的己方义务，不得将己方义务全部或部分转让给第三方完成。否则，乙方所得收益归甲方所有，同时甲方可据此解除本约定书，另给甲方造成损失的，该损失由乙方承担。

4. 除本合同另有约定外，乙方违反合同其他约定，经甲方催告后 5 日内仍拒

不改正的或改正仍不符合本合同要求的，乙方应按合同总金额 5%的比例向甲方支付违约金，甲方有权解除合同，乙方应退还甲方已支付的全部费用，剩余款项甲方不予支付。

5. 乙方违反本合同约定的知识产权条款约定或保密条款的，乙方所得收益归甲方所有，并且乙方还应向甲方支付合同总金额 30%的违约金，违约金无法弥补甲方遭受损失的，乙方还应予以赔偿，甲方有权解除合同。

6. 乙方提供服务不符合本合同约定标准或甲方要求的，乙方应当向甲方支付合同总金额 10%的违约金并在甲方规定的期限内进行返工、修改，并重新提交甲方验收;如乙方提供的服务经二次验收考核仍未通过甲方验收或乙方拒绝按照甲方要求进行返工、修改的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并另行向甲方支付服务费总额 10%的违约金。

7. 无论有无其他约定，本项目中，若导致甲方遭受任何索赔、追诉、处罚的，乙方应当赔偿甲方由此遭受的一切损失，包括但不限于索赔或处罚的金额、律师费、诉讼费用、甲方采取补救措施支出的费用等。

8. 双方就合同的履行产生争议期间，甲方有权暂停向乙方支付相应款项，待争议结束后根据实际情况再行支付且不承担任何违约责任。

9. 本项目乙方不得以任何形式进行转包或分包，甲方如发现乙方对本项目进行转包或分包，甲方有权要求乙方整改，并且乙方应向甲方支付合同总金额 30%的违约金，甲方有权解除合同。

第二条　适用法律

本合同适用中华人民共和国法律（但不包括港、澳、台地区法律）。

第三条　争议解决

1. 执行本合同所发生的与本合同有关的争议，双方应通过友好协商解决。

2. 如果双方通过友好协商不能达成协议，任何一方应当向甲方住所地有管辖权的人民法院提起诉讼。

3. 在争议处理过程中，除正在协商的部分及本合同另有约定外，合同的其它部分继续执行。

第七章　廉政承诺

1. 合同双方承诺共同加强廉洁自律、反对商业贿赂。

2. 甲方及其工作人员不得索要礼金、有价证券和贵重物品:不得在乙方报销应由本单位或个人支付的费用:不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬:不得参加乙方安排的超标准宴请和娱乐活动。

3. 乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品:不得为其报销应由甲方单位或个人支付的费用;不得向甲方工作人员支付劳务报酬:不得安排甲方工作人员参加超标准宴请及娱乐活动。

第八章　其他约定

第一条　不可抗力

1. 不可抗力是指不能预见、不能避免并不能克服的客观情况，如地震、台风、洪水等自然灾害。

2. 在本合同约定的履行期内，如出现不可抗力直接影响本合同的履行或者导致双方不能按照约定履行合同的，遇有不可抗力的一方可以免除相关合同责任。但是遇有不可抗力的一方应立即书面通知对方，并在 15 天之内提供上述不可抗力的详细情况及合同不能履行或者部分不能履行或者需要延期履行的理由和有效的证明文件。按照不可抗力对履行合同影响的程度，由双方协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。一方迟延履行本合同时发生了不可抗力的，迟延方的合同义务不能免除。受不可抗力影响的一方，应当尽可能采取合理的行为和适当的措施减轻不可抗力对履行本合同所造成的影响。没有采取适当措施致使损失扩大的，该方不得就扩大损失的部分要求免责或赔偿。

3. 本合同所称不可抗力包括：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害，以及本合同各方不可预见、不可防止并不能避免或克服的一切其他事件

第二条　合同条款的可分性

如果本合同及其附件项下的任何条款被有权机关判定为无效或不具有可执行性，并不影响本合同及附件的其他条款的有效性和可执行性，除非前述无效或不可执行根本导致了本合同目的无法实现。

第三条　其他事项

1. 合同一式肆份，双方各执贰份，具有同等法律效力。

2. 其他约定：乙方提供的运维服务符合甲方的实际需求。

3. 服务范围、内容及要求：以招标文件、投标文件为基础，满足采购人使用要求（招标文件、投标文件与合同具有同等法律效力），服务方案、应急预案等内容以乙方投标文件为准。

4. 本合同附件与本合同具有同等法律效力。附件 1：分项报价表 附件 2:验收考核细则

（以下无正文）

甲方：北京中医医院顺义医院

法定代表人或授权代表：

日　　期2025年12月17日

乙方：北京金瑞亿科技有限公司

法定代表人或授权代表：

日　　期2025年12月17日

附件 1：分项报价表

序号	分项名称	单价（元/年）	数量	合价（元/年）	备注/说明
1	集成运维巡检	2000	12 次/年	24000	全年 12 次，每月 1 次
2	威胁情报分析	2500	12 次/年	30000	全年 12 次，每月 1 次
3	脆弱性检查服务	4000	2 次/年	8000	全年 2 次，每半年 1 次
4	安全加固服务	6500	2 次/年	13000	全年 2 次，每半年 1 次
5	差异化分析服务	4000	1 次/年	4000	全年 1 次
6	网络安全检查	20000	全年	20000	根据甲方要求
7	风险评估服务	6000	1 次/年	6000	全年 1 次
8	安全管理体系建设	2000	1 次/年	2000	全年 1 次
9	渗透测试服务	6000	4 次/年	24000	全年 4 次，每季度 1 次
10	应急响应	20000	全年（含应急预案完善）	20000	根据实际情况提供应急响应服务（包含应急预案完善）
11	应急演练	5000	1 次/年	5000	全年 1 次
12	重保值守服务	20000	全年	20000	重保期间值守服务
13	安全培训	3000	1 次/年	3000	全年 1 次
14	驻场运维服务	230000	1 人/年	230000	全年 1 人次，工作日 5*8 小时值守
15	设备资产管理、配置	3000	全年	3000	根据甲方要求
16	网络调整优化	2000	全年	2000	根据甲方要求
17	操作系统调整优化	2000	全年	2000	根据甲方要求
18	设备维护更换、优化	2000	全年	2000	根据甲方要求
总价（元/年）				418000	

附件2：验收考核细则

一、总则

1. 目的为加强网络安全运维管理，保障网络系统的稳定运行和数据安全，提高运维人员的工作积极性和责任心，特制定本考核细则。

2. 考核原则坚持公平、公正、公开的原则，以客观事实为依据，以量化指标为重点，全面、准确地评价运维公司的工作及运维人员的日常工作。

二、考核指标体系

（一）工作业绩（60 分）

1. 设备与系统维护（20 分）

• 设备巡检与监控（12 分）

• 巡检计划执行情况：按照既定的巡检计划，对网络设备（如路由器、交换机、防火墙等）、安全设备（如入侵检测系统、漏洞扫描系统等）以及服务器等关键设备进行定期巡检。每少完成一次巡检扣 1 分。

• 巡检记录完整性：巡检记录应详细记录设备的运行状态、性能指标、异常情况等信息。记录不完整或存在虚假记录，每次扣 1 分。

• 监控系统有效性：监控系统应实时监测网络和系统的运行状态，及时发现异常情况并发出警报。若因监控系统故障或设置不当导致未能及时发现安全问题，每次扣 2 分。

• 设备故障处理（8 分）

• 故障响应时间：对于一般故障，应在接到通知后 30 分钟内响应；对于重大故障，应在 15 分钟内到达现场进行处理。每超时一次扣 2 分。

• 故障解决效率：在规定时间内成功解决故障，恢复设备正常运行。若故障未能在规定时间内解决，每次扣 3 分；因故障处理不当导致故障扩大或影响业务正常运行，每次扣 5 分。

2. 安全漏洞管理（15 分）

• 漏洞扫描与发现（5 分）

• 定期开展漏洞扫描工作，按照要求对网络系统、应用系统等进行全面扫描。每少进行一次扫描扣 2 分。

• 及时发现并记录新出现的安全漏洞，若因未及时发现漏洞导致系统遭受攻击或数据泄露，每次扣 5 分。

• 漏洞修复与验证（10 分）

• 制定详细的漏洞修复计划，按照计划及时修复发现的安全漏洞。高危漏洞修复率应达到 90%，中危漏洞修复率不低于 95%。每有一个高危漏洞未修复扣 5 分，每有一个中危漏洞未修复扣 2 分。

• 对修复后的漏洞进行验证，确保漏洞已彻底修复且不影响系统正常运行。若验证不通过，每次扣 2 分。

3. 数据备份与恢复（15 分）

• 备份策略执行（7 分）

• 按照制定的数据备份策略，定期对重要数据进行备份及查看。每少进行一次备份扣 2 分。

• 备份数据应存储在安全可靠的位置，确保数据的完整性和可用性。若因备份数据存储不当导致数据丢失或损坏，每次扣 5 分。

• 恢复测试与演练（8 分）

• 定期进行数据恢复测试，验证备份数据的可恢复性。每少进行一次恢复测试扣 3 分。

• 组织开展数据恢复演练，提高应对数据丢失等突发事件的能力。每少组织一次演练扣 5 分。

4. 应急响应与处置（10 分）

• 应急预案制定与更新（3 分）

• 制定完善的网络安全应急预案，明确应急处置流程和责任分工。预案内容不完整或不符合实际需求，扣 2 分。

• 根据网络环境和业务变化，及时更新应急预案。未及时更新预案，每次扣 1 分。

• 应急演练与效果评估（4 分）

• 定期组织应急演练，检验应急预案的可行性和有效性。每少组织一次演练扣 2 分。

• 对演练效果进行评估，总结经验教训，提出改进措施。未进行演练效果评估，每次扣 2 分。

• 突发事件处置（3 分）

• 在发生网络安全突发事件时，能够迅速响应，按照应急预案进行处置，有效控制事件影响范围。若因处置不当导致事件扩大或造成严重后果，每次扣 3 分。

（二）工作能力（20 分）

1. 专业知识与技能（8 分）

• 具备扎实的网络安全专业知识，熟悉常见的网络安全技术和工具。通过相关专业考试或获得相关认证（如 CISSP、CISP 等），加 3 分。

• 能够熟练运用各种安全工具进行漏洞扫描、渗透测试、日志分析等工作。若因技能不足导致工作失误或效率低下，每次扣 2 分。

2. 问题解决能力（6 分）

• 能够独立分析和解决网络安全运维过程中遇到的问题。对于复杂问题，能够提出有效的解决方案并组织实施。若在规定时间内未能解决问题且未及时向上级汇报，每次扣 3 分。

• 善于总结经验教训，对常见问题进行归纳整理，形成知识库或操作手册，提高工作效率和质量。每完成一份有价值的知识文档，加 2 分。

3. 团队协作能力（6 分）

• 能够与团队成员密切配合，共同完成网络安全运维任务。在团队项目中，积极参与讨论和协作，为团队目标的实现贡献力量。若因个人原因导致团队协作不畅，每次扣 2 分。

• 能够与其他部门进行有效的沟通和协调，及时解决涉及网络安全的问题。若因沟通不畅导致工作延误或出现矛盾，每次扣 2 分。

（三）工作态度（20 分）

1. 责任心（8 分）

• 对工作认真负责，严格遵守工作纪律和规章制度。若因工作疏忽导致安全事故或数据泄露，每次扣 5 分。

• 主动承担工作任务，不推诿、不扯皮。对于上级安排的工作任务，能够按时、高质量地完成。若未按时完成任务且无正当理由，每次扣 3 分。

2. 主动性（6 分）

• 具有较强的工作主动性，能够主动关注网络安全动态，及时了解新的安全威胁和防护技术，并提出改进建议。每提出一条有价值的建议并被采纳，加 2 分。

• 主动参与网络安全相关的培训、学习和交流活动，不断提升自身的业务水平。每参加一次相关活动，加 1 分。

3. 服务意识（6 分）

• 树立良好的服务意识，积极为甲方提供网络安全方面的支持和帮助。若因服务态度不好导致甲方投诉，每次扣 3 分。

• 对甲方反馈的问题能够及时响应和处理，提高甲方满意度。若甲方满意度调查结果低于 90%，扣 3 分。

三、验收标准

考核结果总得分≥95分视为考核合格。但当考核指标中“工作业绩“项扣分≥1分，则视为验收未通过。