政府采购合同（货物）

合同编号：

项目名称：南京市江宁医院终端、服务器安全加固与管理项目

项目编号：JSZC-320115-JZCG-G2025-0043

甲方（买方）：南京市江宁医院

乙方（卖方）：联通数字科技有限公司

甲、乙双方依据《中华人民共和国民法典》、《中华人民共和国政府采购法》等有关的法律法规，以及本采购项目采购文件(征集文件)、乙方的《投标(响应)文件》及《中标(成交)通知书》，签署本合同。

一、合同内容

1.1 标的名称：南京市江宁医院终端、服务器安全加固与管理项目

序号	产品名称	品牌	规格或型号	交付期	数量	单位	单价(元)	总价(元)
1	终端防护软件	绿盟	绿盟终端安全管理系统 ESSNX1-SNM	60 天	1	套	360000	360000
2	服务器防护软件	绿盟	绿盟终端安全管理系统 ESSNX1-SNM	60 天	1	套	178000	178000
3	堡垒机	网御星云	LA-OS-7500-MYJ	60 天	1	台	85800	85800
4	内外网安全隔离设备	绿盟	绿盟防火墙系统 NFNX5-HDX2000	60 天	2	台	86000	172000
5	负载均衡	网御星云	Leadsec-ADC200-N2500	60 天	2	台	105000	210000
6	IT 基础设施运维管理平台	智先生	智维·网络运维管理系统	60 天	1	项	980000	980000
（大写）：壹佰玖拾捌万伍仟捌佰圆								

乙方应严格按照本合同约定提供物资设备及相应技术服务，上述列表清单未尽事宜，详见本合同附件所约定的物资设备技术参数及要求等具体条款。

1.2 标的质量：按招标文件及投标文件执行。

1.3 标的数量（规模）：按招标文件及投标文件执行。

1.4 履行时间（期限）：交货期为合同签订之日起60天内（合同签订后30天内：完成全部货物到货，甲方完成到货验收；到货后15天内：完成所有设备安装、系统部署与调试；调试完成后15天内：进入试运行阶段，试运行期不少于30天），质保期为自交货完成且竣工验收合格之日（竣工验收证书签发日期）起5年。

1.5 履行地点：南京市江宁医院

1.6 履行方式：乙方需在合同签订后3个工作日内，向甲方提交《项目履约对接表》，明确项目负责人（姓名、电话、邮箱）、技术负责人及应急联系人，确保7×24小时响应。

（1）乙方负责设备到场后的卸货、搬运（至甲方指定场地），并承担相关费用；

（2）安装前需提交《安装调试方案》（含施工时间、人员配置、安全防护措施），经甲方书面确认后方可实施；

（3）乙方需保障新设备与甲方现有IT系统（如医院HIS系统、办公系统）的兼容性，调试阶段需完成不低于3次兼容性测试，测试报告经甲方签字确认；

（4）调试完成后 10 个工作日内，乙方需为甲方提供不少于 2 场培训（含设备操作、日常维护、故障排查），培训对象覆盖机房管理员、科室使用人员（不少于10人）；

（5）培训后需提交《培训签到表》《培训考核报告》，确保甲方人员能独立完成设备日常操作与基础故障处理。

1.7 包装方式：按招标文件及投标文件执行。

1.8 合同文件的优先顺序

组成合同的各项文件应互相解释，互为说明。解释合同文件的优先顺序如下：

（1）合同协议书；

（2）中标通知书；

（3）中标文件；

（4）招标文件；

（5）有关技术标准和要求；

（6）其他合同文件：本合同附件包括的《产品技术参数确认表》《安装调试方案》《验收标准及流程》《培训计划》，与本合同正文具有同等法律效力。附件内容与正文冲突的，以正文为准；正文未提及的，以附件为准。”

上述各项合同文件包括合同当事人就该项合同文件所作出的补充和修改，属于同一类内容的文件，应以最新签署的为准。

在合同订立及履行过程中形成的与合同有关的文件均构成合同文件组成部分，并根据其性质确定优先解释顺序。

二、合同金额

2.1 本合同金额为（大写）：壹佰玖拾捌万伍仟捌佰圆（1985800元）人民币。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供货物(包含与货物相关的服务)的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。保密期至保密内容按照相关法律法规规定，以合法方式和途径将其全部披露或本合同终止后5年为止，以两者孰长为准。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同货物（包含与货物相关的服务）或其任何一部分时不受第三方提出侵犯其专利权、著作权、商标权、工业设计权、商业秘密等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的货物（包含与货物相关的服务）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 本项目乙方无需缴纳履约保证金。

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 除招标文件接受分包并经甲方同意，乙方可按分包意向协议分包情况外，乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权终止合同。

八、合同款项支付

8.1 合同款项的支付方式及时间

8.1.1 合同签订后，甲方支付合同总价款的 30%作为预付款。

8.1.2 供货验收（到货验收）合格、安装调试完成且通过产品功能测试后，甲方收到乙方发票后，甲方支付合同总价款的 40%。

8.1.3 完成试运行且项目竣工验收合格，甲方收到乙方发票后，支付合同总价款的 20%。

8.1.4 质保期 5 年内，每年质保服务完成且甲方评估合格后，甲方收到乙方发票后，每年支付合同金额的 2%。

8.1.5 满足合同约定支付条件的，甲方收到乙方发票后，将资金支付到合同约定的乙方账户。

8.2 根据《保障中小企业款项支付条例》规定，甲方未按合同约定支付款项的，乙方可以向有关部门投诉。

8.3 当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

九、税费

9.1 本合同执行中的相关税费均由乙方负担。

十、质量保修范围和保修期及售后服务

10.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

10.2 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商可按以下方式处理：

10.2.1 更换：由乙方承担所发生的全部费用。

10.2.2 贬值处理：由甲乙双方合议定价。

10.2.3 退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

10.3 如在使用过程中发生质量问题，乙方应在接到甲方通知后 2 小时内响应、4 小时内到达甲方现场、2 个工作日解决问题。

10.4 质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

10.5 质保期为自交货完成且竣工验收合格之日（竣工验收证书签发日期）起5年，因人为因素出现的故障不在质保范围内。超过质保期的乙方负责终生维修，维修时只收取部件成本费。

十一、项目验收

11.1 甲方依法组织履约验收工作。

11.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案做好相应配合工作。

验收阶段	验收时间	验收内容	验收标准
到货验收	货物到场后 3 个工作日内	1. 设备数量、品牌、型号与合同一致； 2. 设备外观无破损、配件齐全； 3. 随货技术资料(合格证、说明书等）完整	1. 对照合同附件《产品清单》逐一核对； 2. 外观无划痕、变形，配件无缺失； 3. 技术资料需含纸质版（2 份)+ 电子版(U 盘）
中期验收	安装调试完成后 5 个工作日内	1. 设备安装位置符合甲方要求； 2. 系统功能测试（如终端防护软件的病毒查杀、堡垒机的权限管控等）	1. 安装位置与《安装调试方案》一致； 2. 所有功能测试项 100%通过（测试项详见附件《技术参数确认表》）
竣工验收	试运行 30 天后 5 个工作日内	1. 试运行期间设备无故障（故障定义：单次停机超1 小时或月停机超3次）； 2. 乙方响应及时（2小时内到场，24 小时内解决一般故障） 3.合同约定事项完成情况。	1.试运行报告无故障记录； 2.乙方服务记录完整，甲方无异议 3.乙方按合同要求完成服务，符合竣工要求。

11.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

11.4 如有必要，甲方可邀请参加本项目投标的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收结论的参考。

11.5 甲方成立验收小组，按照采购合同约定对乙方履约情况进行验收。验收时间、验收标准见招标文件。验收时甲方按照采购合同的约定对每一项技术、商务要求的履约情况进行确认。验收结束后验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金退还挂钩。履约验收的各项资料存档备查。

11.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

11.7 任一验收阶段不合格，乙方需在5个工作日内提交《整改方案》，整改期间甲方提供电力、网络等必要支持，整改期限不超过10个工作日。若因非可归责于乙方的原因导致同一阶段整改超过2次仍不合格，双方应友好协商解决。协商不成双方解除合同，乙方已完成部分合同工作并能达到部分安全加固合同目的的可协商按完成部分工作量与合同总价比例支付对应款项。若确属乙方原因，甲方有权解除合同。要求乙方返还预付款，乙方投入的设备、软件由乙方回收。

十二、货物的包装、发运及运输

12.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。货物的包装应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的规定。

12.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

12.3 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

12.4 货物在交付甲方前发生的风险均由乙方负责。

12.5 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

十三、违约责任

13.1 甲方无正当理由拒收货物的，应向乙方偿付拒收货物总价款 5% 的违约金。

13.2 甲方无故逾期验收和办理货款支付手续的，应按逾期付款总额每日万分之五向乙方支付违约金。

13.3 乙方逾期交付货物的，应按逾期交货总额每日万分之五向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本

合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，应向甲方支付合同总价 5% 的违约金。

13.4 乙方所交付的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

13.5 甲乙双方任何一方违反本合同约定的，除应承担上述违约责任外，违约方还应当赔偿因此给守约方造成的一切直接和间接损失，包括但不限于守约方的实际损失、预期可得利益损失以及为实现债权而产生的费用（包括但不限于诉讼费、保全费、保全担保费、律师费、公证费、鉴定费、差旅费）。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件（包括自然灾害、战争、政策调整等）导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

14.2 不可抗力事件发生后，应立即通知对方并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续 120 天以上，双方应通过友好协商确定是否继续履行合同。

十五、解决争议的方法

15.1 甲乙双方因合同签订、履行而发生的一切争议，应通过友好协商解决。协商不成的由甲方住所地人民法院管辖。

十六、合同生效及其它

16.1 本合同经双方加盖单位公章后生效。

16.2 本合同未尽事宜，遵照《中华人民共和国民法典》《中华人民共和国政府采购法》有关条文执行。

16.3 本合同正本一式陆份，具有同等法律效力，甲方叁、乙方各执叁份。

甲　方：南京市江宁医院（公章）　　乙　方：联通数字科技有限公司（公章）

地　址：　　地　址：

法定代表人或授权代表：　　法定代表人或授权代表：

联系电话：　　联系电话：

签订日期：2025.12.10

附件 1：

货物（产品）需求参数一览表

项目名称：南京市江宁医院终端、服务器安全加固与管理项目

项目编号：JSZC-320115-JZCG-G2025-0043

序号	货物名称	数量	品牌	型号	招标文件需求参数
1	终端防护软件	1 套	绿盟	ESSNX1-SNM	1、完全满足招标文件中：提供不少于 5 人（防护软件实施）的部署小组，并在终端防护软件安装后 60 天内完成医院指定终端的病毒查杀软件部署任务。
					2、完全满足招标文件中：提供 3200 点终端客户端软件和管理控制台授权。功能模块包含：病毒防护、虚拟补丁、检测及响应 EDR、资产管理、漏洞管理、外设管控。
					3、完全满足招标文件中：在质保服务期间，根据医院终端设备的变动情况，完成杀毒软件的新机安装和授权迁移等工作。
					4、完全满足招标文件中：资产管理：支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看。
					5、完全满足招标文件中：终端自防护：黑客工具防御，包含：xuetr、ProcessHacker、PCHunter、Mimikatz 等工具自启动。
					6、完全满足招标文件中：勒索病毒专防：通过实时监测异常行为，发生勒索事件时，实现文件动态备份，自动删除原始文件夹中被加密的文件夹并隔离文件。
					7、完全满足招标文件中：联动响应：支持与现有上网行为管理平台（深信服品牌）进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。
					8、完全满足招标文件中：入侵攻击行为检测：支持不同攻击阶段的主要攻击手法检测，对包括但不仅限于以下攻击手法精准检测：执行、持久化、权限提升、防御逃逸、凭证窃取、横向移动等攻击手法检测记录。显示事件详情，展示攻击手法对应的高危操作和威胁实体。
					9、完全满足招标文件中：终端资产盘点：协助医院信息人员，对医院 3200 点终端设备（如电脑、打印机、医疗专用设备等）进行资产盘点，完成资产台帐工作。
					10、完全满足招标文件中：软件部署：对医院 3200 点终端设备（如电脑、打印机、医疗专用设备等）完成杀毒软件的安装部署配置，重点关注门诊、药房、检验科等高频使用区域的设备，以及连接互联网的终端。
					11、完全满足招标文件中：恶意软件（代码）清除：结合产品自带杀毒软件警告，人工参与识别并清除病毒、木马、勒索软件、间谍软件等恶意程序，恢复被篡改的系统文件和设置。针对医疗设备专用软件，需避免误删关键文件，必要时与厂商技术人员协同处理。
					12、完全满足招标文件中：系统漏洞修复：结合产品自带杀毒软件提示，检查操作系统、杀毒软件、业务软件的补丁更新情

					况，手动安装官方发布的安全补丁，关闭高危端口（如 445、135 等）。对不支持自动更新的老旧设备（如部分医疗仪器），需评估风险后手动修复漏洞或采取隔离措施。
					13、完全满足招标文件中：网络环境排查：检查医院局域网内设备的联网状态，识别异常连接（如未经授权的接入设备），排查 ARP 欺骗、DNS 劫持等网络攻击迹象，排查单机同时接入内网和外网的情况。
					14、完全满足招标文件中：数据备份与恢复支持：确认关键数据（如电子病历、检验报告、影像资料等）的备份机制是否正常，协助恢复被病毒破坏的数据（需在杀毒完成后操作）。指导医护人员定期手动备份重要文件，避免因病毒导致数据丢失。
					15、完全满足招标文件中：应急响应处置：针对突发病毒事件（如大规模勒索软件感染），立即隔离感染设备，启动医院信息处应急预案，记录病毒特征并上报医院信息处。配合医院信息处追溯病毒传播路径（如邮件附件、U 盘接入、网页挂马等），防止二次扩散。
					16、完全满足招标文件中：设备安全加固：对终端设备进行安全配置优化，如启用系统自带防火墙、禁用自动播放功能、限制普通用户权限、设置强密码策略等。对公共区域设备（如导诊台电脑、自助服务终端），需定期重置系统或恢复初始状态，防止恶意软件驻留。
					17、完全满足招标文件中：移动存储管理：检查全院移动存储设备（U 盘、移动硬盘等）的使用情况，禁止未经杀毒的设备接入内网。对医护人员因工作需要使用的存储设备，提供免费病毒扫描服务，并建立登记制度。
					18、完全满足招标文件中：每次服务后填写《病毒查杀工作报告》，记录扫描设备数量、病毒类型、处理结果及建议。定期与医院信息处沟通，反馈病毒趋势及系统薄弱环节，协助制定长期安全防护策略。
2	服务器防护软件	1 套	绿盟	ESSNX1-SNM	1、完全满足招标文件中：提供不少于 5 人（防护软件实施）的部署小组，并在服务器防护软件安装后 60 天内完成医院指定终端的病毒查杀软件部署任务。（此处 5 人与终端防护软件部署人员可重复）
					2、完全满足招标文件中：提供 300 点服务器终端客户端软件和管理控制台授权。功能模块包含：病毒防护、虚拟补丁、检测及响应 EDR、资产管理、漏洞管理、外设管控。
					3、完全满足招标文件中：在质保服务期间，根据医院终端设备的变动情况，完成杀毒软件的新机安装和授权迁移等工作。
					4、完全满足招标文件中：服务器加固：针对 windows 服务器，提供 RDP 远程登录保护，开启 RDP 远程登录二次认证，针对 Linux 服务器，提供 SSH 远程登录保护，开启 SSH 远程登录二次认证。
					5、完全满足招标文件中：勒索病毒专防：提供勒索行为检测手段，对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截。
					6、完全满足招标文件中：漏洞防护：针对 Windows 高危漏洞，支持轻补丁防御。
					7、完全满足招标文件中：支持管理员在现有的上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止

					病毒进一步扩散。
					8、完全满足招标文件中：VPT 漏洞排序：支持结合漏洞自身属性、外部漏洞情报以及资产暴露面等多个维度，进一步消减高危漏洞数量，对发现的漏洞进行优先级排序，包含响应、关注、观察 3 种结果。
					9、完全满足招标文件中：终端资产盘点：协助医院信息人员，对医院 300 点服务器终端设备进行资产盘点，完成资产台帐工作。
					10、完全满足招标文件中：软件部署：对医院 300 点服务器终端设备完成杀毒软件的安装部署配置，重点关注门诊、药房、检验科等高频使用区域的设备，以及连接互联网的终端。
					11、完全满足招标文件中：恶意软件（代码）清除：结合产品自带杀毒软件警告，人工参与识别并清除病毒、木马、勒索软件、间谍软件等恶意程序，恢复被篡改的系统文件和设置。针对医疗设备专用软件，需避免误删关键文件，必要时与厂商技术人员协同处理。
					12、完全满足招标文件中：系统漏洞修复：结合产品自带杀毒软件提示，检查操作系统、杀毒软件、业务软件的补丁更新情况，手动安装官方发布的安全补丁，关闭高危端口（如 445、135 等）。对不支持自动更新的老旧设备（如部分医疗仪器），需评估风险后手动修复漏洞或采取隔离措施。
					I3、完全满足招标文件中：网络环境排查：检查医院局域网内设备的联网状态，识别异常连接（如未经授权的接入设备），排查 ARP 欺骗、DNS 劫持等网络攻击迹象，排查单机同时接入内网和外网的情况。
					14、完全满足招标文件中：数据备份与恢复支持：确认关键数据（如电子病历、检验报告、影像资料等）的备份机制是否正常，协助恢复被病毒破坏的数据（需在杀毒完成后操作）。指导医护人员定期手动备份重要文件，避免因病毒导致数据丢失。
					15、完全满足招标文件中：应急响应处置：针对突发病毒事件（如大规模勒索软件感染），立即隔离感染设备，启动医院信息处应急预案，记录病毒特征并上报医院信息处。配合医院信息处追溯病毒传播路径（如邮件附件、U 盘接入、网页挂马等），防止二次扩散。
					16、完全满足招标文件中：服务记录与反馈：每次服务后填写《病毒查杀工作报告》，记录扫描设备数量、病毒类型、处理结果及建议。定期与医院信息处沟通，反馈病毒趋势及系统薄弱环节，协助制定长期安全防护策略。
3	堡垒机	1 台	网御星云	LA-OS-7500-MYJ	1、完全满足招标文件中：提供不少于 2000 点资源管理授权的硬件设备。
					2、完全满足招标文件中：并发会话数性能要求：支持≥800 图形并发和 1500 字符并发。
					3、完全满足招标文件中：2U 标准硬件；硬盘：≥16TB；内存≥16G；电源：冗余电源；网络接口≥2 个千兆电口。
					4、完全满足招标文件中：支持对 Windows、Linux、Unix、网络及安全设备、数据库以及各类 B/S 应用的管理。
					5、完全满足招标文件中：支持管理 IPv6 资产。
					6、完全满足招标文件中：支持 Web、Mstsc、SSH Client 等多种访问模式，支持批量启动功能，可一次性登录指定目标设备。

					7、完全满足招标文件中：支持以 EXCEL 方式批量导入资源系统账号及密码，支持资源账号密码托管，实现应用系统单点登录功能，支持系统账号密码触发式校验功能，对托管的口令进行验证。
					8、完全满足招标文件中：能够实时显示在线会话、在线字符会话、在线图形会话、在线数据库会话，能够直接点击查看审计会话。
					9、完全满足招标文件中：支持图形智能审计，可在审计回放界面上，同步显示关键的键盘操作、标题栏操作、剪贴板操作等文字信息，并能在点击任意文字信息，可直接定位到相关画面。
					10、完全满足招标文件中：支持基于 A/B 角管理模式的双人复核，当用户登录到设定的重要目标设备或者是执行高危命令，必须经过复核人的复核确认后才能正常操作；当会话复核人发现操作存在风险，可实时暂停会话。
					11、完全满足招标文件中：支持本地密码、AD/LDAP、RADIUS、动态令牌、手机令牌、USBKey、短信、X.509 等认证方式，支持双因素组合认证，可以将两种认证方式自定义组合为全新的认证方式（如本地密码+手机令牌）
4	内外网安全隔离设备	2 台	绿盟	NFNX5-HDX2000	1、完全满足招标文件中：形态：标准 2U 硬件设备，配置冗余电源，端口≥8 个千兆电口，2 个千兆光口，4 个万兆光口。
					2、完全满足招标文件中：性能：吞吐率≥20Gbps，并发连接数≥1000 万，最大并发连接数（防火墙+APP+AV+IPS）≥500 万，每秒新建≥10 万/秒。
					3、完全满足招标文件中：提供五年 IPS 特征库授权、AV 特征库授权、应用识别特征库授权、URL 库授权。
					4、完全满足招标文件中：虚拟化：支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。
					5、完全满足招标文件中：访问控制：支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
					6、完全满足招标文件中：恶意文件检测：支持对恶意文件的检测，阻断、日志上报。支持手动添加恶意文件 hash。支持恶意文件库的自动升级和离线导入。支持手工添加、删除恶意文件特征。
					7、完全满足招标文件中：弱口令检查：支持对服务器、客户端进行的口令暴力破解的攻击防护；
					8、完全满足招标文件中：Web 应用防护：支持独立的 WEB 特征库，并可以自动、手工升级；
					9、完全满足招标文件中：资产防护：支持通过主动及被动探测方式，识别终端类型（至少包括：PC、网络打印机、网络摄像机、网络设备、防火墙、负载均衡等），支持多种资产异常告警选项包括 MAC 地址、操作系统、厂商、类别、指纹等。支持资产行为画像，通过资产的连接关系、应用、应用流量、并发连接等的图形化展示；支持对资产的行为学习，自动学习资产相关的流量以及网络连接关系，通过连接关系拓扑可以进行阻断、一键生成安全策略操作；
					10、完全满足招标文件中：SD-WAN：支持数据压缩功能，采用

					标准的压缩算法来压缩数据，从而减少传输数据量并降低带宽消耗，缩短客户端访问的下载等待时间。支持双边加速。
					11、完全满足招标文件中：产品架构：多核并行增强安全操作系统，非传统单核架构。
5	负载均衡	2台	网御星云	Leadsec-ADC200-N2500	1、完全满足招标文件中：形态：标准 1U 硬件设备；配备冗余电源；接口≥6 千兆电口+2 千兆光口。
					2、完全满足招标文件中：性能：4 层吞吐量≥5Gbps；4 层并发连接数≥800 万；4 层新建连接数 CPS≥15 万；7 层新建连接数 RPS≥10 万。
					3、完全满足招标文件中：单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能，三种功能同时处于激活可使用状态，无需额外购买相应授权。
					4、完全满足招标文件中：国产化兼容：支持 OceanBase、达梦、南大通用、人大金仓和 TDSQL 数据库的负载均衡。
					5、完全满足招标文件中：IPv6 改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题。
					6、完全满足招标文件中：负载均衡算法支持：支持加权轮询、加权最小连接、加权最小流量、最小流量、最少连接算法等。
					7、完全满足招标文件中：内置规则库：支持基于应用协议的智能选路，内置网上银行、Web 流媒体、游戏、音频视频规则库，并且规则库不少于 5000 条。
					8、完全满足招标文件中：连接限制：支持节点设置并发连接限制、新建连接限制、每秒请求限制和上下行流量限制；HTTP 检查 支持 HTTP 的被动健康检查。
					9、完全满足招标文件中：动态负载均衡：根据服务器的实时负载情况动态地调整请求的分发策略。可以根据服务器的 CPU 利用率、内存使用情况等指标来进行动态负载均衡。
					10、完全满足招标文件中：SSL 算法：支持配置 SSL 服务为单向、双向国际算法的 SSL 服务端。
					11、完全满足招标文件中：系统可靠性要求：提供冗余高可用架构部署方式，支持在单设备故障时，业务能够自动切换到另一个设备中继续运行，无需人工干预。
6	IT基础设施运维管理平台	1项	智先生	智维·网络运维管理系统	1、完全满足招标文件中：提供 IT 基础设施运维管理平台软件 1 套，提供 IT 基础设施运维管理平台人工智能服务器 1 台。
					2、完全满足招标文件中：提供的 IT 基础设施运维管理平台软件部署需求：包含自动网络发现、拓扑管理、告警管理、IP 地址管理、自动巡检等组件。网络监控节点授权≥900 节点包括交换机、路由器、防火墙数据库、中间件等；无线资源监控授权≥2300 点；业务视图≥30 个。
					3、完全满足招标文件中： 提供的 IT 基础设施运维管理平台人工智能服务器部署，配置不低于： 1）CPU：≥2*Intel Xeon Gold 6530 32C 2.1Ghz 160MB 270W XCC； 2）内存：≥32*32GB DDR5-5600 ECC REG RDIMM； 3）硬盘：≥2*960GB SATA R SSD，≥4*3.84TB NVMESSD； 4）GPU：≥8*Tesla L20 48G PCI-e； 5）网卡：≥双口 25G 网卡含万兆多模模块。扩展卡：VROC

					套件支持 NVMe SSD RAID 0/1/5，12Gb 3808 8i Raid0 1 00 10 JBOD 半高； 6）电源：≥4*2700w； 7)性能:支持不少于 100 并发,总推理速度不少于 150-300 tokens/s。
					4、完全满足招标文件中：监控工作台：实现面向业务的监控，展示所有业务当前的运行情况和关联的资源数；实现接入的监控资源总体情况，包括正常设备数、严重设备数、提醒设备数、失联设备数等；实现系统接入的设备数及各种设备类型的接入数，包括操作系统、数据库、中间件、网络设备、服务器、存储设备等；展示最新严重告警信息，能够快捷定位需要处理的告警事件。
					5、完全满足招标文件中：综合监控：展示监控对象的总体概况，包括监控资源的基本信息、核心指标、实时状态和实时告警信息；根据告警级别、发生时间等条件查询监控对象的全部告警信息；快速切换当前业务系统的其他监控对象；实现展示监控对象的全部指标列表；支持所有监控对象显示在一个列表中，清晰地看到每类监控对象的数量和通过关键字快速查找；支持针对具体监控对象的监控指标和触发器的管理。
					6、完全满足招标文件中：操作系统监控：支持 Windows、Linux、麒麟、统信等国产操作系统的监控，支持主动和被动两种方式；支持对 CPU 使用率、CPU 负载、队列长度、CPU 系统态使用率的监控；对内存使用情况监控；提供磁盘预计用完时间；支持对网络发送与接收速率、丢包率、错误包数、网卡流量进行监控；支持对进程、端口和服务进行监控。分析进程占用内存和 CPU 的相关情况，如：进程 CPU 占用前二十，进程内存占用前二十等；支持对支撑业务系统正常运行的重要端口、服务、进程的可用性进行监控。
					7、完全满足招标文件中：数据库监控：支持 Caché数据库、TiDB、MySQL、SQLServer、Oracle、PostgreSQL、 DBMongoDB、Redis、ElasticSearch、达梦数据库的监控；
					8、完全满足招标文件中：中间件监控：支持对 Nginx、IIS、Tomcat、WebLogic、Resin、Apache、Zookeeper、Jboos、东方通 TongWeb 中间件的监控；支持对 ActiveMQ、RabbitMQ、Kafka 等消息队列的监控；支持对 Zookeeper、Kafka 集群进行监控；支持中间件的请求、会话、类、线程、堆内存、垃圾回收和资源等进行监控。
					9、完全满足招标文件中：虚拟化监控：支持虚拟化平台的监控，包括虚拟化平台的宿主机、集群、虚拟机等监控；支持虚拟化平台的总体情况展示，包括虚拟机的开关机情况、宿主机的开关机情况、CPU\硬盘\内存的总体使用情况、虚拟机 CPU 使用率和内存使用率前五等；支持主机视图和虚拟机视图两种树状维度，清晰显示虚拟化平台的架构：支持虚拟机视角监控，包括虚拟机的 IP、状态、CPU 使用率、内存使用率、磁盘使用率、CPU 核数、内存大小等；支持监控虚拟机和宿主机的状态、CPU、内存、磁盘等基础信息。
					10、完全满足招标文件中：网络设备监控：支持对不同品牌交换机、防火墙、入侵防护、上网行为、负载均衡、网闸、防毒墙、邮件安全等安全设备的监控；支持对不同品牌交换机端口状态、流量监控分析功能；支持对不同品牌交换机电源、风扇、

					电源、主板等硬件监控，CPU、内存的性能监控；支持对不同品牌的 AC 控制器和 AP 无线终端设备监控；支持 SNMP V1/V2/V3 版本的兼容。平台支持对核心、汇聚、接入层交换机的网络拓扑（包含子拓扑）的自动发现、自动生成拓扑图功能；支持对重要端口（级联端口或其他重要端口）可以手动添加监控信息，如果出现重要端口连接中断可及时报警。
					11、完全满足招标文件中：物理服务器监控：支持对华为、戴尔、华三、惠普、联想、浪潮等各品牌物理服务器的监控；支持对跨平台（Windows、Linux、Unix）操作系统级指标项的监控；支持对物理服务器的硬件监控，包括风扇、温度、电源、电池、电流、电压和主板等。
					12、完全满足招标文件中：存储监控：支持对惠普、日立、EMC、群晖、IBM、华为等各平台物理存储设备的监控；支持读取存储池和物理硬盘信息，支持对存储的分析，包括发送数、错误硬盘数、Autosupport 发送成功数等；支持读取存储的网口状态、速率，以及流量等信息；支持获取存储的背板和节点信息。
					13、完全满足招标文件中：调用链监控：支持端到端管理，支持监控服务调用延迟、QPS、错误日志、调用链等信息监控；自动生成业务调用链，无需人工干预并可将发现的中间件自动纳入监控系统中。
					14、完全满足招标文件中：API 监控：支持对 API 的连通性、可用性、延迟等指标监控；支持使用定时请求、日志、抓包、旁听、Agent 方式监控；支持根据优先级对 API 监控告警；支持手动添加 WEB 地址，并对其地址访问情况进行监控。同时系统支持对 WSDL 地址可用性进行监控。
					15、完全满足招标文件中：智能提醒：支持在移动端使用接收告警和在线查看监控详情，移动端处理告警；支持短信、钉钉机器人、企业微信机器人、邮件等各种通知媒介的方式进行告警；支持消息的订阅，按照监控对象分发给不同的运维人员；支持根据设备级别发给不同的人员；告警支持设备等级的差异化通知，包括通知方式等；移动端所有页面，都可以由用户自定义配置，而不需要修改源代码，支持水平模式，垂直模式，两种方式展示。
					16、完全满足招标文件中：业务展示：支持按业务系统分类等保级别、网络类型等多维度树状展示；支持展示业务系统关联资源的所有告警信息；支持对全院业务系统健康状况报警、提醒、正常的直观展示，支持对业务报警进行逐层下钻；对业务所关联服务器的性能、系统、网口、配置、日志的报警展示，支持运维笔记、文档管理及支撑业务运行的所有软硬件报警、提醒、恢复、笔记等全方位时间轴展示；支持业务系统告警影响范围查看，支持切换告警关联业务拓扑图；实现与工单、巡检闭环管理。
					17、完全满足招标文件中：资源合理度分配分析：支持全网服务器、虚拟机资源的 CPU、内存、硬盘资源的分配情况及分配合理度进行分析，同时支持台账导出功能。实现与资产闭环管理；支持全网服务器、虚拟机资源的 CPU、内存周平均使用率分析，预判预计可使用天数，同时支持台账导出功能；支持设备速查功能，可以快速查询单台服务器的资源配置情况、使用情况、合理度分析三个维度在同一个页面内的直观对比展示.
					18、完全满足招标文件中：需求快速响应能力：具有极速开发

					效率，既智能又灵活快速响应业务，不用修改源代码即可实现客户需求；在应用软件中可以直接创建的所有表和 er 实体关系模型，不需要操作后台数据库，随时添加字段，并修改字段类型，自动更新数据库，内置字段达 5 个以上；全面的可视化设计和开发支持，包括应用基本架构、服务、数据、代码、页面等，都能完全可视化、拖拽式设计，系统自带组件，控件。通过拖拉点拽方式进行设计，可支持各种表格、曲线、折线图、柱状图，页面中支持嵌入 groovy 脚本语言，设计完成后，系统可以自动生成源代码，源代码保存在服务器数据库中，无需重新部署即可立即生效运行，支持 json 源码的导入与导出。
					19、完全满足招标文件中：提供 AI 软件/平台/工具部署：安装算力管理平台/模型管理平台软件，支持 GPU 监控、池化、切分、资源开通、任务发布调度、基础权限管理能力。
					20、完全满足招标文件中：提供 GPU 资源生命周期管理、计算任务调度、GPU 资源监控和算力隔离服务、日志管理、监控告警管理的软件部署。
					21、完全满足招标文件中：根据医院要求，预置 DeepSeek70B 模型（Int8 量化）、Qwen、Llama 等开源模型的一种或多种及基础问答、知识库、模型仓库应用。

附件 2:

安全生产承诺书

设备/软件安装(含维修)单位的消防、安全生产、治安管理工作责任人在南京市江宁医院的指导下，全面负责本单位相关设备/软件安装(含维修)期间的消防、安全生产和治安防范工作，履行下列职责：

一 、贯彻执行消防法规、建筑法规、安全治安管理有关法律法规，自觉接受信息管理部门的安全管理领导。

二、设备/软件安装(含维修)管理必须坚持“安全第一、预防为主”的方针，软件安装(含维修)单位的法定代表人对本单位在南京市江宁医院的安全生产负责。

三、设备/软件安装(含维修)单位必须依法加强对医疗设备安全施工的管理，执行安全生产责任制度，采取有效措施，防止伤亡和其他安全生产责任事故的发生。

四 、设备/软件安装(含维修)单位应当建立健全劳动安全生产教育培训制度，加强对职工安全生产的教育和培训，未经安全生产教育培训人员不得上岗作业。

五、设备/软件安装(含维修)的施工人员在南京市江宁医院的施工过程中，应当遵守有关安全生产的法律、法规和建筑行业、医疗设备行业的安全规章(规程)，不得违章指挥 或违章作业。

六、设备/软件安装(含维修)单位应当在施工现场采取维护安全、防范危险、预防火灾等措施，施工现场对毗邻的建筑、构筑物、其他设备和特殊作业环境可能造成伤害的，设备/软件安装(含维修)单位应当采取措施加以保护。设备/软件安装(含维修)单位在施工现场应注意对现场施工人员、医护人员、就诊患者及家属的安全防护，做好场地围挡、现场维护 。

七、设备/软件安装(含维修)单位应加强对在南京市江宁医院施工的工程人员的管理， 并将在我单位施工的所有工作人员名单上报到南京市江宁医院信息管理部门备案，接受甲方 动态监督。

八、设备/软件安装(含维修)单位因违反上述规定引起事故、造成人员伤亡及财产损失的，由设备/软件安装(含维修)单位负全部责任，并承担受损单位的经济赔偿责任，对屡教不改的设备/软件安装(含维修)单位，甲方有权中止采购合同。

九、请认真阅读以上规定，签字(盖章)后，表示已同意遵守甲方有关消防、安全生产、 治安保卫规定，甲方对本制度有最终解释权。

软件安装(维护)单位(章)：

法定代表人(签字)：

日期： 年 月 日

附件 3:

南京市江宁医院单位物资购销廉洁条例

为进一步加强医疗卫生行风建设，规范医疗卫生机构购销行为，有效防范商业贿赂 行为，营造公平交易、诚实守信的购销环境，甲方特制定本条例，以资医疗卫生机构购 销双方共同遵守：

1. 合同双方按照《中华人民共和国民法典》及购销廉洁条例约定购销设备和服务等 行为。

2. 甲方应当严格执行采购和服务合同验收、入库制度，对采购产品及发票进行查验， 不得违反有关规定合同外采购、违价采购或从非规定渠道采购。

3. 甲方严禁接受乙方以任何名义、形式给予的回扣，不得将接受捐赠资助与采购挂 钩。甲方工作人员不得参加乙方安排并支付费用的营业性娱乐场所的娱乐活动，不得以 任何形式向乙方索要现金、有价证券、支付凭证和贵重礼品等。被迫接受乙方给予的钱 物，应予退还，无法退还的，有责任如实向本单位纪检监察部门反映情况。

4. 甲方严禁利用任何途径和方式，为乙方个人提供便利。

5. 乙方不得以回扣、宴请等方式影响甲方工作人员采购或使用产品的选择权，不得 在为甲方人员提供旅游、超标准支付食宿费用。

6. 乙方指定人员必须在工作时间到甲方指定地点联系商谈，不得借故到甲方相关领 导、部门负责人及相关工作人员家中访谈并提供任何好处费等。

7. 乙方如违反本廉洁条例， 一经发现，甲方有权立即终止购销合同，并向市卫生行 政部门报告。如乙方被列入商业贿赂不良记录，则严格按照《国家卫生计生委关于建立 医药购销领域商业贿赂不良记录的规定》（国卫法制发〔2013〕50 号)相关规定处理。

8. 本廉洁条例为甲方产品和服务购销行为的廉洁准则，双方均需严格遵守。

9. 本条例由甲方负责解释。

甲方：（公章）

日期：2015 年 1 月 10 日

乙方：（公章）

附件 4:

信息安全与保密协议

甲方：南京市江宁医院　　乙方：联通数字科技有限公司

鉴于乙方拟向甲方提供南京市江宁医院信息技术服务，在服务过 程中双方存在信息交流共享和资料的提供等情形，为确保信息系统安 全与保密，甲方与乙方达成如下保密协议：

一、保密内容

甲方的保密信息包括但不限于：

甲方的业务数据，包括患者信息、医疗记录、医院员工信息、运 营数据等；

甲方的网络拓扑、系统架构、配置信息、安全策略等；

甲方的系统弱点、安全漏洞、风险评估报告等；

甲方的系统和设备管理信息，包括账户、密码、访问权限等；

甲方的管理制度及记录，包括操作规程、维护日志、事故处理记 录等；

双方在合作过程中产生的任何其他保密信息。

二、保密义务

1. 乙方在信息系统运维过程中，对上述内容负有严格的保密责任和 义务，未经甲方授权，不得向第三方透露。乙方不得将从信息系统中 得到的信息用于甲方之外的任何商业目的。

2. 乙方应确保其员工遵守本协议的保密条款，并对其员工的违约行 为承担责任。

三、保密期限

本协议约定的保密义务具有持续性，不因双方合作的结束而终止。 保密信息的保密期限为本协议签订之日起至保密信息已公开或经提供方书面许可公开为止。

四 、信息安全措施

乙方应采取必要和合理的信息安全措施，包括但不限于物理安全、 网络安全、数据安全等，以保护甲方的保密信息不被非法访问、使用、 泄露、丢失或被篡改。

五、违约责任

乙方如违反本协议规定，给甲方及患者个人造成任何损失或伤害，乙方应当采取有效措施防止保密信息进一步被泄露，并承担相应的法 律及经济责任。同时，甲方有权向乙方追究法律责任。

六、协议效力

本协议书与维护合同具有同等法律效力， 一式陆份，甲、乙双方各执叁份，经双方签字盖章后生效。

甲　方：南京市江宁医院（公章）

地　址：

法定代表人或授权代表：

联系电话：

乙　方：联通数字科技有限公司（公章）

地　址：

法定代表人或授权代表：

联系电话：

签订日期：2025.12.10