**南方科技大学医院信息化项目论证**

**用户需求书**

1. 项目背景

近年来，随着“互联网+医疗健康”战略的深入推进，南方科技大学医院的信息化建设已全面覆盖电子病历（EMR）、医院信息系统（HIS）、医学影像系统（PACS）等核心业务，并逐步向智慧医院、互联网医疗方向发展。然而，随着网络规模的扩大和接入终端的多样化，医院面临日益严峻的网络安全挑战。

终端接入风险：移动医疗设备（如PDA、智能输液泵）、物联网终端（如智能门禁、环境监测设备）、第三方运维设备等大量接入医院内网，缺乏统一认证和访问控制，可能成为攻击者渗透的入口。

运维安全隐患：IT运维人员、外包服务商等通过高权限账户直接访问核心服务器、数据库，缺乏细粒度权限控制和操作审计，存在数据泄露、误操作或恶意篡改风险。

合规性要求：根据《网络安全法》《数据安全法》《医疗卫生机构网络安全管理办法》及等保2.0三级要求，医院需建立网络边界防护、终端准入控制、运维操作审计等安全机制。

为全面提升医院网络安全防护能力，保障业务系统稳定运行，医院计划实施网络安全加固项目，重点部署网络准入控制系统（NAC）和运维堡垒机（跳板机），构建“终端可信接入+运维安全管控”的双重防护体系。

1. 项目建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 单位：项 | 备注 |
| 1 | 南方科技大学医院网络安全加固项目 | 1 |  |

1. 项目建设内容

|  |  |  |
| --- | --- | --- |
| **名称** | **功能** | **详细技术要求** |
| 网络终端准入控制系统 | 1.身份认证 | 对接入内网的终端进行安全准入控制，必须通过管理员审核才能接入网络。 |
| 2.IP/MAC绑定 | 对内网终端设备进行IP/MAC绑定，防止私自更改IP和MAC地址，防止外来非法终端盗用合法IP地址使用内部网络。 |
| 3.设备类型绑定 | 设备类型绑定，确定IP终端设备的唯一性，防止非法用户利用瘦客户机或其他IP设备网络接口入网。 |
| 4.资产可视化管理 | 自动发现并识别网内所有的接入终端信息，包括不同操作系统的PC终端和不同类型的哑终端，能够根据终端类型进行自动分类统计，形成完整的终端资产台账。 |
| 运维保垒机 | 1.双因子认证 | 为了提高来源身份的可靠性，提供USBKEY、手机APP认证（谷歌动态口令验证）、双因素认证引擎，提供短信认证、AD、LDAP、RADIUS认证的接口，支持多种认证方式同时使用、多种认证方式组合使用实现二次登录认证，防止身份冒用。 |
| 2.全面的资产运维 | 支持管理Linux服务器、Unix服务器、Windows服务器、网络设备、文件服务器、Web系统、数据库服务器等，所有数据中心的设备均支持运维。 |
| 3.多种运维方式 | 为满足不同运维人员的运维习惯，提供 B/S运维、C/S运维、H5运维、专用运维客户端（支持UOS /麒麟等国产操作系统）、应用发布运维和网关隧道运维六大运维方式，提供更加灵活的运维方式。 |
| 4.访问权限控制 | 提供主机资产及数据库的运维命令管控，可提供针对设定命令的命令审批、阻断命令、中断会话及直接放行等不同管理措施，加强运维管理力度，防止恶意违规和运维误操作。 |
| 5.精准的审计溯源 | 提供事件检索、录像审计、OCR文字提取和数据库图形文字双向审计，全面记录运维过程中的所有操作。 |

1. 项目预算说明

根据建设内容给出项目申请预算表或给出市场询价报告(不限于其他医院类似项目的合同价，相关网站类似项目中标价或咨询相关厂家报价)。