**终端安全管理和网络准入控制系统**

**需求文档**

# 投标要求

**“★”号标注项为必备指标要求，不满足将导致投标被拒绝**

★为避免出现兼容性问题，提升售后维护效率，要求准入控制系统和终端安全管理系统为同一厂商产品，使用一个客户端代理程序即可完成所有功能，从而减少终端资源占用，减轻维护工作量。（提供产品销售许可证作为证明，并加盖厂商公章）。

★所有投标产品均需提供产品原厂商针对本项目的授权函。

★签订合同前甲方有权对投标产品功能按照参数要求逐一验证，若不符合要求，甲方有权拒绝签订合同。

## 系统技术要求

## 系统成熟、稳定

* 系统须保证“7天24小时”安全运行。
* 产品成熟，并经过运行考验，有同等规模医院成功运行经验。

## 系统安全

1）数据库的安全性

* 数据库有完善备份功能。
* 数据定期备份，并支持备份到独立的数据中心或磁带库，有备份记录。
* 系统有完备的断点恢复功能，终端离线再接回网后数据可以继续上报。
* 提供重要数据修改全程监控。
* 对于重要数据，系统只能提供有痕迹的更正功能。
* 提供错误日志。
* **★系统具有直观全面的日志管理模块，对系统的运行进行全面的日志记录与管理，确保系统运行的安全性与可追溯性。（提供软件截图证明）**

2）授权管理

* 完善的用户权限管理与授权机制。
* 不同权限进入不同层次、功能的菜单。
* 系统提供操作权限管理工具，无需通过修改程序进行授权。
1.

## 系统可升级

* 系统可升级，并有统一、方便的升级方式。

## 信息安全与数据保密

* 注重信息安全，保证系统安全性，严格防止信息泄漏。
* 具有数据保密功能。
* 符合信息安全等级保护规范要求。

## 数据集成要求

要求能够与医院现有报警平台及资产管理系统对接，能够通过syslog、webservices等通用格式将告警信息发送至报警平台，将终端资产信息发送到资产管理系统（此项无需另行付费）。

## 数据接口

* 接口原则：保持数据一致性、保持数据的完整性、保持数据库的效率、数据库的安全性。
* 需要实现短信平台和待建系统的数据接口。

应有用户自定义程序接口，使用户在不修改主程序前提下而能实现客户化的功能。

## 售后服务与实施

## 实施

* 合理的、具有针对性的项目实施计划与解决方案。
* 负责完成客户化工作，满足招标文件要求的功能需求，同时还应满足实施过程中医院提出的具体需求，及时响应与完成客户化修改。
* 能够妥善分析医院业务中的复杂问题与个性化问题，并提出合理的解决方案，以保证系统实施不做弯路。
* 项目组织机构完整，保证实施期间有充分的实施技术人员保障，上线期间现场常驻工程师。
* 项目负责人与参与项目实施技术人员具有相关实施经验。
* 具有规范的项目组织与项目管理体系与方法。

## 整体系统安装、调试

* 负责服务器、操作系统、数据库、应用服务器、中间件及客户端支持软件、应用软件整体安装调试
* 系统出现问题时负责诊断、并与其他有关厂商共同协调，解决问题。

## 维护

* 自验收之日起提供3年免费维护。
* 终身负责维护、升级。
* 产品具备应急机制，当设备发生故障时，对终端入网、使用均无影响，或能在5分钟内恢复终端正常使用。
* 系统出故障时做到24小时随时响应，技术人员现场响应时间≤１小时。
* 提供各种技术文档资料,在投标书中列明所提供的文档资料清单。

## 培训（此项费用不另行付费）

* 培训，包括数据库与技术培训、系统维护培训、高级用户培训、用户培训，并保证培训效果。
* 出具详细的培训计划书。
* 提供培训教材

## 售后服务承诺

* 出具售后服务承

# 终端安全管理系统技术指标要求

## 系统总体技术要求

1. ★系统客户端支持部署在： WindowsXP、Win7、Win8、Win10系统的32位和64位。
2. ★系统管理端支持部署在：Windows server2003、 Windows server 2008、Windows server 2012系统。
3. 系统无使用期限限制。
4. #具备国家版权局颁发的计算机软件著作权登记证书
5. #公安部监制的计算机信息系统安全专用产品销售许可证
6. #国家保密局科技测评中心颁发的涉密信息系统产品检测证书
7. 授权数：最少支持管理3000个终端

## 基本管理

1. 策略管理：系统支持根据用户和根据设备两种模式的策略下发，还可根据用户所在组、IP地址、操作系、统、自定义检索等多种方式进行策略分发。
2. 策略采用下载到本地执行的方式，断网重连后终端再次获取最新策略，同时上报离线期间审计记录。终端安全程序可自动侦测网络连接情况，根据连接内网/未连接内网可执行不同的安全策略。
3. 具备独立审计账户、管理账户，权限各自独立。提供系统运行审计和操作审计机制，系统管理员登录要求支持IP地址访问限定，只有获得授权的计算机才能进入系统控制台。
4. 具备服务器自我保护功能，可以防止IP占用、DDos攻击，具备支持10000台以上终端管理能力。
5. 客户端功能在安全模式下仍生效。
6. 系统必须具备良好的系统安全性，终端具有自我防护机制，防止用户使用网上常见的卸载等工具随意停止、卸载。
7. 支持用户自定义报表的内容及报项，支持Word、Excel等多种格式的文件导出。

## 资产管理功能

* 1. 系统要求支持管理网络终端软硬件资产，包括硬件设备信息、位置信息（设备名称、使用人、联系电话、所属部门等）、网络信息（MAC地址、IP地址等）、软件安装信息（操作系统、应用软件）等，支持手动修改和添加硬件信息。
	2. #硬件变化管理：系统要求支持设备硬件变化行为报警；支持对未注册设备、注册程序卸载行为的报警。
	3. #系统兼容Intel vPro主动管理技术。（需提供功能截图，并加盖厂商公章）

## 终端管理功能

1. 终端支持代理软件和IE代理禁用功能。
2. 要求支持网管统一管理的主机防火墙功能。
3. #支持进程管理功能：支持对（包括软件厂商名、源文件产品名、源文件名、进程名等）的进程进行黑白名单的控制，黑名单内进程自动被禁止，白名单内进程自动启动。（需提供功能截图，并加盖厂商公章）
4. 外设控制功能：可控制硬件外设的使用，启用或禁用3G网卡、光驱、USB全部接口、 串行口、并行口、1394控制器、无线网卡和其他不常用接口等等；支持禁用自定义设备。
5. 消息通知功能：可分区域、时间进行，可强制用户查看。
6. 支持远程点对点管理功能，如运行进程、开放端口、补丁查看、终端安全审计、共享目录检查、远程卸载客户端程序、远程断开/恢复网络连接等。
7. 支持IP与MAC绑定，禁止终端用户修改IP地址、网关等参数，并自动恢复、断网和提示等处理。
8. 支持远程屏幕接管功能。
9. 具备远程对终端的网络数据包协议分析。
10. 终端服务管理：查询当前终端运行的服务，可远程关闭或开启服务。
11. 垃圾文件清理
12. 管理员可在控制台对终端用户某一文件夹下或全盘某些后缀的垃圾文件或临时文件进行集中清理。
13. 日志查询：查看终端的系统日志、安全日志和应用程序日志。
14. 修改网络配置：可查看网络终端的IP、MAC、子网掩码和网关信息，并可远程修改用户的IP地址。

## 安全管理功能

1. 具备主流厂商杀毒软件运行监测功能，并进行提示或断网处理。能够监测杀毒软件是否及时更新。
2. #具备注册表监控/保护功能，实现注册表安全管理。（需提供功能截图，并加盖厂商公章）
3. 终端统一防火墙：理员在控制台可对终端进行统一的防火墙设置，对网络IP及协议访问进行限制。
4. 终端在线/离线策略管理：针对不同的网络接入情况，设定终端的在线、离线策略。

## 安全运维功能

1. 能够对终端的CPU、内存、硬盘的资源占用率和剩余空间进行监控，设定危险等级报警阈值。
2. 具备对客户端流量的控制和采样，能够设定终端流量阈值。
3. #可定期自动将客户端指定文件备份到服务器、支持增量备份。（需提供功能截图，并加盖厂商公章）
4. 进程异常监控：在控制台对终端未响应窗口进行监控并结束或重启该进程，对意外退出的进程进行监控和保护。

## 违规联网监控功能

1. #系统支持违规联网监测和取证功能，可发现内网设备违规联入互联网的行为，并进行报警和阻断，审计终端违规外联的路由情况。（需提供功能截图，并加盖厂商公章）
2. #支持在互联网部署的外网报警服务器，终端违规接入互联网后自动与服务器通信，上报终端信息，实现违规外联强审计和抗抵赖。（需提供功能截图，并加盖厂商公章）。

## 随身wifi管控功能

1. #支持wifi热点使用管理，具备允许或禁止开启wifi热点共享功能，支持外接随身wifi和笔记本共享wifi的管控。（需提供功能截图，并加盖厂商公章）
2. #支持wifi热点接入管理，手机或笔记本电脑通过内网终端共享的wifi接入时对其进行验证，允许合规的设备通过共享wifi接入网络，禁止非法设备接入。（需提供功能截图，并加盖厂商公章）
3. #支持对单位内的wifi管理功能，能够审计单位内所有wifi信号，支持管理允许接入的wifi和禁止接入的wifi白/黑名单。（需提供功能截图，并加盖厂商公章）

## 移动存储介质管理功能

1. 支持U盘、移动硬盘、存储卡等存储设备注册管理。
2. 注册登记与加密处理。对于处于敏感信息的移动存储介质，在使用之前需进行登记注册和加密处理。登记信息包括：使用人、使用部门、联系电话等等。
3. 支持对移动存储介质信息进行统计查询。可按照不同部门、不同使用人、标签等进行分类统计，并导出。
4. 用户无法通过分区或格式化等操作进行破解。
5. 注册后的U盘采用标签认证，区分不同的网络使用范围。新注册的U盘无需在系统中全网下发序列号，通过标签认证直接使用。
6. #支持多标签管理，相互隔离网络的U盘可写入不同的标签，杜绝不同网络之间U盘交叉使用。（需提供功能截图，并加盖厂商公章）
7. #支持标签U盘双分区。（需提供功能截图，并加盖厂商公章）
8. 系统支持多标签管理，同一网络不同部门的U盘可写入不同的标签，从而实现同一网络不同部门之间U盘交叉使用的权限控制。
9. 支持移动存储设备管理白名单，以便数码相机等移动存储设备临时接入
10. 数据保护。已注册的移动存储介质只能在本网络的授权终端使用，否则设备不可用，确保数据安全。
11. 可以制定策略使已注册的移动存储介质在外部环境（即终端离线状态）中将完全不可用，即使是已授权的用户和终端设备。
12. 使用行为审计。已注册的移动存储介质的整个使用过程均会被记录并上传至管理服务器。

## 主机安全审计功能

1. #支持对设定目录文件的操作审计，包括文件创建、打印、读写、复制、改名、删除、移动等的记录，同时将信息上报管理信息库供查询；具备对终端的系统、软件和共享等目录中的文件具有保护功能，设定访问、删除、修改权限；支持全盘文件禁止删除，审计自定义文件扩展名。（需提供功能截图，并加盖厂商公章）
2. 具备对用户的网页访问行为进行控制并对用户访问的网页进行本地审计和记录上报。能够设置访问域名或IP的黑白名单。
3. 具备禁止、审计将文件拷贝到网络盘的操作行为，能够监测拷贝文件的文件名及内容是否包含敏感字，可禁止用户拷贝包含敏感字的文件。（需提供功能截图，并加盖厂商公章）
4. 具备对主机发送的邮件进行审计，支持常用web邮箱及Foxmail等客户端形式的邮件审计。
5. 具备对主机所有打印行为进行监控审计，可审计使用人、部门、打印时间、打印文档路径及名称。可设置关键字，当打印包含关键字的文档时禁止输出。能够备份打印的文件到服务器上以备审查。
6. #具备对主机刻录行为进行管理和审计的功能，能够审计终端刻录行为，客户端集成专用刻录软件，自动屏蔽其他刻录软件和系统自带刻录功能，只能通过专用软件刻录；具备普通刻录和封口刻录的功能；刻录前需要输入操作人的账号密码以验证身份。（需提供功能截图，并加盖厂商公章）
7. 具体审计用户/组权限更改，操作系统内用户/组的增、删操作。
8. 具备对系统日志、应用日志、安全日志审计和读取查看功能。

## 报表管理功能

1. 系统可提供多种完善的报表功能。
2. 具有查询功能，能根据不同的需要进行多种不同条件组合，可生成多种不同的报表格式。
3. 报表可以网页的方式呈现，并可以以Excel等格式输出。
4. 系统可以生成柱形图、饼图等，一目了然的展现报表信息。

## 事件报警管理

1. 可汇总所有内外安全管理事件的报警信息，并将报警按种类、级别分类，同时支持短信、声音、邮件、图形等报警方式。
2. 客户机发给管理服务器相关的报警信息可预设置级别，可将部分紧急的报警信息发送给管理员。
3. 对客户机的不当行为，管理服务器可按照预先制定的策略自动进行警告。

## 补丁及文件分发功能

1. 具备补丁自动分发安装，同时支持默认和用户自定义补丁分发策略，并自主配置分发。
2. #具备终端代理转发技术，未下载补丁的终端可从已下载补丁的终端获取补丁，从而缓解服务器压力，提高补丁分发效率。（需提供功能截图，并加盖厂商公章）
3. 具备终端补丁查询功能，终端用户可以在网络上查找自身漏打补丁的详细信息，并进行补丁下载安装；管理员也可远程检测终端补丁安装状况。
4. 具备补丁的增量更新导入。
5. 具备终端补丁最大连接限制和最大流量控制。
6. 具备补丁安装情况与未打补丁情况汇总统计。
7. #具备补丁内网自动测试功能，即用户可自主选定内网部分设备为补丁安装测试设备，系统将新获得的补丁自动发送给这些设备，在测试设备安装指定时间间隔后再自动分发给其他设备。（需提供功能截图，并加盖厂商公章）
8. 具备文件分发功能，能自动向终端分发各类文件和可执行程序，支持后台静默安装和运行分发的程序。
9. #能够通过文件、进程等信息判断分发的程序是否下载并安装成功，能够统计文件分发结果。（需提供功能截图，并加盖厂商公章）
10. 支持统计分发程序的安装情况。
11. 支持文件代理转发功能，减轻服务器和网络压力。

# 准入控制系统产品功能

## 系统总体技术需求

1. 1. 准入控制产品为软硬件一体机，软硬件均为同一厂商。
2. 实配至少4个千兆业务接口，支持可扩展2个万兆网络业务光接口。（需提供设备面板照片并加盖厂商公章）
3. 实配1个console接口，实配独立双机热备心跳接口。（需提供设备面板照片并加盖厂商公章）
4. 实配液晶屏，支持显示的信息包括但不限于设备IP地址、系统时间、CPU使用率、内存使用率。（需提供设备面板照片并加盖厂商公章）
5. 授权数：最少支持管理5000个终端
6. 部署方式：支持集中部署、分级部署两种模式。
7. 自主产品：产品须具备软件著作权证书。（需提供产品著作权证书复印件并）
8. 产品证书：具备销售许可证（需提供产品著作权证书复印件并）；具备涉密信息系统产品检测证书（需提供产品著作权证书复印件并）

## 网络发现

1. 支持通过SNMP、SNMP Trap、TELNET、ARP、流量分析等技术扫描发现终端设备。
2. 支持按设备类型分组展示终端信息以及按组织架构拓扑形式展示终端信息；
3. 支持自动发现全网各种私接乱接的AP、交换机、HUB等设备，支持对其阻断、告警；
4. #支持自动发现网络中IP/MAC等伪装仿冒行为，如：PC仿冒哑终端IP/MAC入网、非法PC仿冒合法PC的IP/MAC入网；（需提供产品功能截图并加盖厂商公章）

## 终端识别

1. 支持自动识别全网所有接入终端的IP地址、MAC地址、主机名、网卡厂商、终端类型、操作系统、接入位置、接入时间、接入状态，并全网可视化展示；
2. 内置网络打印机，网络摄像头，指纹机，刷卡器，瘦客户机等专用终端的指纹识别库
3. #支持自动识别并提取、手动添加、修改、管理终端指纹，并支持不少于MAC厂商、操作系统、开放端口等指纹特征，添加后可全网自动匹配实现同类型设备识别并丰富指纹库；（需提供产品功能截图并加盖厂商公章）
4. #终端注册后能够通过客户端实现未注册终端与注册终端的网络隔离，及时网线直连也不能访问（需提供产品功能截图并加盖厂商公章）

## 安全隔离

系统应遵循终端注册->身份认证->安全检查->安全隔离/允许入网的控制流程，对于未通过安全检查的终端，可以采用安全隔离手段将终端进行隔离，被隔离的终端只能访问指定的安全控制域。

## 来宾入网管理

外来访客要求临时性的接入网络时，应对外来访客进行临时授权，并控制外来访客的访问权限。

## 准入控制

1. #支持交换机端口准入、802.1x准入、VLAN隔离准入、旁路镜像准入、策略路由准入、透明网桥准入、DHCP准入、ARP准入等多种准入控制方式，并支持多种准入技术组合使用，应对不同网络环境（需提供产品功能截图并加盖厂商公章）
2. #支持准入策略统一制定、下发部署功能,可根据访问IP源、目的域以及准入流程进行策略制定，目的域需是IP、端口以及目录的组合。（需提供产品功能截图并加盖厂商公章）
3. #支持ARP阻断扩展部署模式，通过小型ARP阻断设备扩展部署，降低成本。（需提供产品功能截图并加盖厂商公章）
4. 支持自动发现采用NAT模式入网的终端并强制认证，支持NAT下的终端进行分别准入认证。（需提供产品功能截图并加盖厂商公章）
5. #要求能够通过特征识别技术防止外部电脑通过网线直连等方式访问内部电脑。（需提供功能截图，并加盖厂商公章）

## 安全域控制

可安全域来控制不同用户不同角色的访问控制域。

## 身份认证

1. #支持portal认证，支持与域联动，实现域账号portal认证，支持portal认证与终端-交换机绑定相结合，认证后自动绑定终端和交换机，实现端口准入控制下的portal认证。（需提供产品功能截图并加盖厂商公章）
2. 支持802.1x认证，认证系统支持本地账户、本地Radius、远程Radius、域账户等。支持与AD域服务器、LDAP服务器实现联动认证。
3. #支持人脸识别认证，具备自主开发的人脸识别功能，无需与第三方人脸识别程序结合，在安装有摄像头的PC终端上可实现人脸识别认证入网。（需提供产品功能截图并加盖厂商公章）
4. #支持通过多元素绑定的方式认证终端身份，包括终端IP、终端MAC、交换机、交换机端口、终端类型，支持任意元素组合绑定的方式认证入网。（需提供产品功能截图并加盖厂商公章）

## 入网认证日志

支持对全网用户的认证情况进行记录，可以详细记录用户认证的时间、用户名、认证类型、IP以及认证动作等。

## 注册管理

1. #支持注册审核管理功能，已注册终端需通过管理员审核通过之后才可以接入网络。
2. #支持中标麒麟等国产操作系统安装客户端。（需提供产品功能截图并加盖厂商公章）。
3. 支持主流windows、linux操作系统终端的程序安装注册。
4. #支持摄像头、打印机、IP电话等哑终端的页面引导注册，如：摄像头WEB注册重定向引导，可通过身份认证成功的PC访问摄像头自动重定向到摄像头注册页面，填写注册信息进行注册（需提供产品功能截图并加盖厂商公章）
5. #支持系统兼容Intel vPro主动管理技术。（需提供产品功能截图并加盖厂商公章）

## 安全检查

1. #支持PC终端的入网安全检查功能，包含杀毒软件安装情况检查、补丁漏洞检查、系统共享资源检查、IE主页修改项检查、安装软件检查、guest来宾帐户启用情况检查、远程桌面启用情况检查、系统启动项检查、密码强度检查、服务检查、进程检查、违规外联检查、浏览器代理检查、操作系统检查、登陆AD域检查、屏保检查、IE插件检查、注册表检查等功能。（需提供产品功能截图并加盖厂商公章）。
2. #支持哑终端的无客户端安全体检功能，能够检查哑终端弱口令、漏洞情况、端口开放情况等。（需提供产品功能截图并加盖厂商公章）

## 系统监控

1. 支持对系统本身业务接口的连接状态以及接口速率进行监控，支持对系统本身的CPU以及内存使用率提供图形化实时监控数据，支持数据自动刷新。
2. 支持分析结果深度钻取功能，对不同状态的终端分析结果进行深度钻取获取终端的IP列表。

## 系统管理

1. 支持自定义系统管理员，支持管理员角色定义，支持三权分立的管理员角色管理。系统管理员负责授权管理、系统监控等准入系统本身的安全管理功能；安全管理员负责接入终端信息、准入控制策略下发、报警事件查看和处理等准入控制相关功能；安全审计员负责所有管理员登录及操作审计等相关功能。（需提供产品功能截图并加盖厂商公章）
2. 支持以网络设备作为对象进行管理权限划分。
3. 支持OEM自定义功能，提供OEM设置接口，管理员可随意更换页面LOGO等信息以满足自身企业化定制要求。
4. 支持设备之间的级联管控，下级系统可将终端设备信息、告警信息、系统状态信息上报至上级系统。上级系统支持在本级制定的管理策略自动下发到下级系统执行。